



## 저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

**Master's Thesis of Wang Yongmin**

**Study of Threshold Switching behavior  
of Pt/HfO<sub>2</sub>/TiN cell and its application  
in True Random Number Generator**

**August 2019**

**Graduate School of Engineering  
Department of Materials Science and Engineering  
Seoul National University**

**Wang    Yongmin**



# Abstract

The novel technologies like the Internet of Things (IoT) raise the security concerns because of the sensitive information they will handle. That makes the random number generator become one important role in the protection of privacy, which could create one unique signature for each party. And the reliability of this kind of authentication highly depends on how random number generator is. Usually pseudo-random number generator (PRNG) strongly depends on its algorithms or codes, which results in the easy attack. Especially for the sequences they generate could be predictable from their seed value that is fed into generator at the start. That makes true-random number generator (TRNG) become the main role in information security.

Memristor can show resistive switching behavior under proper bias conditions, however, the nonuniformity has troubled people to push the next generation memory. This kind of chaos in switching performance results from the stochastic physical characteristics and other complex mechanisms. The

Pt/HfO<sub>2</sub>/TiN memristor shows a large change scale in switching parameters, which is a big problem for memory application, but a great superiority in the area of the random number generator. The electron transportation of this Pt/HfO<sub>2</sub>/TiN memristor, which is explained by trapping / detrapping mechanism, is mainly attributed to trap-assisted-tunneling process. The cell shows threshold switching behavior under a low compliance current due to limited the number of total injected electrons. And the trap-assisted-tunneling mechanism is related with temperature and distance between intrinsically existed traps in oxide layer, resulting in its stochastic delay time and relaxation time.

One true random number generator based this Pt/HfO<sub>2</sub>/TiN memristor is proposed. And in this proposed TRNG, the Pt/HfO<sub>2</sub>/TiN memristor is used as seed provider and plays the role of the entropy source. Its stochastic physical characteristics are fully used by transformation of Linear Feedback Shift Register's feedback function in the new circuit. The 4-stage LFSR structure is used and restructured to achieve one more complex RNG circuit to avoid attacking. The

output from 4-stage LFSR has been collected and digitized by MATLAB coding. The binary output bits have been run in NIST randomness tests. And the data collected from proposed TRNG has passed all 15 National Institute of Standards and Technology randomness tests, indicating Pt/HfO<sub>2</sub>/TiN memristor would be perfect candidate for hardware security application.

**Keyword :** True Random Number Generator, Linear Feedback Shift Register, memristor, Resistive Switching Random Access Memory  
**Student Number :** 2017-23058

# Contents

Abstract.....	i
Contents .....	iv
List of Figures .....	v
Chapter 1. Introduction .....	1
1.1 Overview .....	1
Chapter 2. Investigation of switching behavior of Pt/HfO <sub>2</sub> /TiN memristor using trap-assisted-tunneling mechanism .....	6
2.1 Introduction.....	6
2.2 Experimental Fabrication .....	7
2.3 Switching Mechanism .....	10
2.4 Experimental Verification and Results .....	17
2.5 Summary.....	20
Chapter 3. Random Number Generator .....	23
3.1 Introduction.....	23
3.2 Pseudo-Random Number Generator .....	24
3.3 D Flip-Flop .....	25
3.4 Linear Feedback Shift Register .....	28
3.5 Non-linear Feedback Solutions for LFSR.....	33
3.6 True Random Number Generator.....	38
3.7 Summary.....	39
Chapter 4. TRNG using Pt/HfO <sub>2</sub> /TiN memristor .....	41
4.1 Introduction.....	41
4.2 Design and Simulation.....	42
4.3 Experimental Procedure .....	51
4.4 NIST Randomness Test .....	57
4.5 Results and Analysis.....	68
4.6 Summary.....	72
Chapter 5. Conclusion.....	74
5.1 Summary.....	74
Bibliography .....	78
Abstract in Korean.....	82

## LIST OF FIGURES

Figure 2.1. The structure of Pt/HfO <sub>2</sub> /TiN memristor .....	9
Figure 2.2. The cross-sectional TEM images of PHT device... .....	9
Figure 2.3. I-V curves under compliance current I <sub>cc</sub> =0.5nA of PHT device .....	14
Figure 2.4. (a) circuit diagram of pulse measurement system; (b) pulse switching performance of PHT device with diagram of measurement system .....	15
Figure 2.5. The simplified trap-assisted-tunneling process in PHT device .....	16
Figure 2.6. The distribution of delay time under different temperature and voltage in the PHT device .....	19
Figure 3.1. The work principle of positive-edge-triggered type of D flip-flop .....	27
Table 3.2. The true table of D flip-flop.....	27
Figure 3.3. A 3-stage Fibonacci LFSR with feedback of $G(X) = X^3 + X^2 + 1$ .....	30
Table 3.4. The maximal period of 3-stage LFSR.....	31
Figure 3.5. The feedback function of m-stage Fibonacci LFSR of $G(X) = g_m X^m + g_{m-1} X^{m-1} + g_{m-2} X^{m-2} \dots g_2 X^2 + g_1 X + g_0$ .....	32
Figure 3.6. An n-bit Fibonacci NLFSR.....	36
Figure 3.7. The Geffe generator.....	36
Figure 3.8. The Massey-Rueppel's generator .....	37
Figure 3.9. The Beth-Piper stop-and-go generator .....	37



Figure 4.1. The proposed new circuit of TRNG based on the PHT memristor .....	45
Figure 4.2. The schematic form of 4-stage LFSR used in our TRNG with a feedback function as $G(X) = X^4 + X^3 + 1$ .....	46
Table 4.3. The longest turn of original 4-stage LFSR based on its feedback function of $G(X) = X^4 + X^3 + 1$ .....	47
Figure 4.4. (a) the monitoring point of the new circuit of TRNG based on PHT memristor; (b) the true table of function in proposed TRNG .....	48
Figure 4.5. The simulation circuit diagram in LTspice of the proposed TRNG .....	49
Figure 4.6. The MOSFET structure of proposed TRNG .....	50
Figure 4.7. The real implementation of proposed TRNG on the breadboard (right) and Probe station 2 (left) .....	54
Figure 4.8. The work principle of proposed TRNG.....	55
Figure 4.9. Experimental output waveform of proposed TRNG .....	56
Table 4.10. The NIST randomness test result of proposed TRNG by using memristor .....	71



# Chapter 1. Introduction

## 1.1. Overview

As we know, the Internet of things (IoT) should be able to deal with a huge amount of security-sensitive information. So the demand for restrict access and encrypted data transmission is certainly high. To solve this , many solutions have been studied and proposed, such as implementation of Root-of-Trust (RoT) in hardware. And also nowadays the data sharing in the air is so common , which makes the cryptography really indispensable. In these areas, random number generator becomes one indispensable part in such design for the area of information protection. It can provide the key stream for any authentication process and signatures for security system at hardware level. And the reliability of this kind of authentication highly depends on how random number generator is. Pseudo-random number generator (PRNG) and True-random number generator (TRNG), as the existing random number generators, show very different characteristics. Usually PRNG strongly depends on its algorithms or codes, which result in the easy attack. Especially for the sequences they generate could be predictable from their seed value that is fed into generator at the start. That makes TRNG become the main role in information security.

A key or signature that is hard to guess, or closely impossible for prediction, is considered as random. So usually one sufficient entropy source that contains the randomness from the natural world is supplied to the generator, mostly PRNG. This entropy source works as the randomness source for generator and leads to the true random number[1]. In other word, the quality of the entropy source for random number generator decides how hard to guess the output sequence. If the random source is weak, it will lead to output with potentially guessable property[2]. And this entropy source can be understood as randomness source, or source of unpredictable behavior, it can be collected from your computer systems or noise from the surrounding, which has true randomness[3-5]. However, the modern design of computers have already minimized this kind of uncertainty. Also the true randomness is relatively difficult to define or value. In common there are three mostly used conditions as standard to value the true randomness. They are ①uniformity, which says that occurrence of zero and one of the output sequence should be same; ②scalability, which is to measure the randomness of any extracted subsequences of output; ③consistency[6].

Considering the need of hardware security, we only focus on the hardware entropy source, which usually come from the variation in some gates or the random state of the system. For example,

hardware Root-of-Trust (RoT) contains the memory and executable instructions in a secure area on the main chip. There one part in it is called hardware random number generators. For this kind of application, certainly it will offer better performance in protection with the true random number generator. However, evaluating the true randomness of certain entropy or generator is hard, actually the main reason of difficulty for measuring the randomness is no such sequence form output consist of all possible patterns. So the current techniques for valuing the true randomness are limited.

NIST has published one statistical test suite for random and pseudorandom number generator, which contain some criteria for characterizing the generator. There are 15 tests in it, which are used to determine the feasibility of generator for cryptography. And the 15 testes are designed under consideration of that three standard conditions: ①uniformity; ②scalability; ③consistency. And this statistical test suite determine certain sequence random or not by the value of P-value, that whose value is 1 means sequence has perfect randomness. Usually the comparison of p-value with significance level of your collected data make sense. The significance level depends on the amount of your collected bits. So if the p-value of one sequence for one test, is higher than this significance level , then

this sequences pass this test[6]. That is the way for NIST to judge some sequence.

Memristor can show resistive switching behavior under proper bias conditions, however, the nonuniformity has troubled people to push the next generation memory. This kind of chaos in switching performance results from the stochastic physical characteristics and other complex mechanisms. Nevertheless, considering the true random number generator at hardware level, stochastic phenomena could be used as a certain entropy source if proper design is proposed[22]. That is exactly what we pursue. The Pt/HfO<sub>2</sub>/TiN memristor show a large change scale in switching parameters, which is a big problem for memory application, however, a great superiority in the area of the random number generator.

The new circuit is designed for take full advantage of its random change in delay time and relaxation time. By using Linear Feedback Shift Register, which is commonly applied for PRNG, one best befitting project is got. And this best befitting design provides enough output bits for NIST test. Not only the simple structure, this proposed TRNG also shows great advantage in high compatibility with CMOS fabrication standard due to using high- $k$  dielectric material, HfO<sub>2</sub>, with high resistance controllability[18-21]. Moreover, the electron transport mechanism in fabricated

Pt/HfO<sub>2</sub>/TiN cell, which is explained by trapping / detrapping process, shows higher switching speed and lower power consumption than ionic switching memristor type[23–25]. And a meritorious result is shown as the evidence, which indicates the memristor is a great candidate for random number generator as the entropy source.

# Chapter 2. Investigation of switching behavior of Pt/HfO<sub>2</sub>/TiN memristor using trap-assisted-tunneling mechanism

## 2.1. Introduction

Pt/HfO<sub>2</sub>/TiN structure is well studied as resistance switching memory. HfO<sub>x</sub> based memristor always draws huge attention due to its excellent performance and potential in memory application, like excellent scalability( $\sim 30$  nm<sup>①</sup>) and great endurance ( $\sim 10^{10}$  cycles) and so on. Also, the structure is often built by stacking AlO<sub>x</sub> or ZrO<sub>x</sub> to improve its uniformity[5–6]. There are different mechanisms for explaining the switching behavior between high resistance state (HRS) and low resistance state (LRS) of HfO<sub>x</sub> based memristor. For metal oxide RRAM, the conduction nature also can be explained by various opinions, such as Poole–Frenkel emission, the Schottky emission or the electron trapping/detrapping process. We fabricated HfO<sub>2</sub> layer with 10 nm thickness, and this structure shows threshold switching performance under relatively low compliance current. Also it brought us a miraculously random change in reaction of electric stimuli.

---

□ Nano-meter



## 2.2 Experimental Fabrication

The Pt/HfO<sub>2</sub>/TiN cell is fabricated with a crosspoint device structure with  $6 \times 6 \mu\text{m}^2$  electrode area. The SiO<sub>2</sub>/Si substrate is used. Then a TiN layer with 50 nm thickness as bottom electrode is deposited by using one sputtering system (Endura, Applied Materials). And 10 nm HfO<sub>2</sub> film is fabricated by ALD thermal atomic layer deposition, using Hf[N(CH<sub>3</sub>)(C<sub>2</sub>H<sub>5</sub>)]<sub>4</sub> as HF precursor and O<sub>3</sub> an oxygen source. the deposition conditions are 8 in. diameter scale traveling-wave-type ALD reactor (CN-1 Co, Plus 200) at 280 °C substrate temperature. At last, the top electrode, Pt layer, is deposited by electron-evaporation to 50 nm thickness through a 120  $\mu\text{m}$  hole diameter metal shadow mask. Then after lift-off with the single crossbar pattern, the Pt/HfO<sub>2</sub>/TiN cell is got, as Figure 2.1 shows.

And this structure is verified by the cross-sectional image obtained from a transmission electron microscope (TEM), as shown in Figure 2.2. The threshold switching behavior was tested by a voltage sweep under a compliance current of 0.5 nA during the electronforming step and set process at room temperature, and the testing equipment is one semiconductor parameter analyzer (Hewlett-Packard, HP4145B). The pulsed measurement is also applied on Pt/HfO<sub>2</sub>/TiN device by using Agilent 81110A PG pulse

generator to observe the delay effect and relaxation effect of the whole switching process.

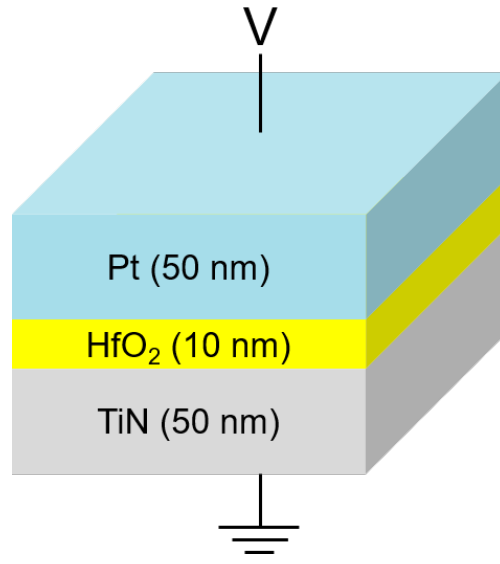


Figure 2.1. The structure of Pt/HfO<sub>2</sub>/TiN memristor. The TiN layer with 50 nm thickness as bottom electrode, 10nm-thick HfO<sub>2</sub> layer as oxide film, Pt layer is deposited to 50 nm thickness as top electrode.

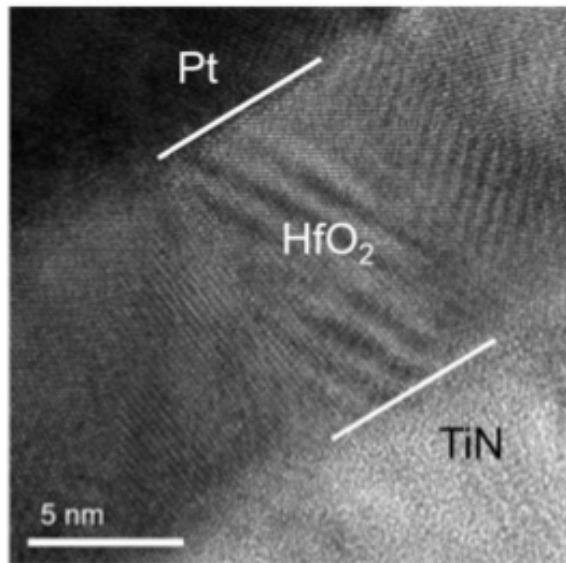


Figure 2.2. The cross-sectional TEM images of PHT device, with a 10nm thick HfO<sub>2</sub> layer sandwiched in Pt and TiN metal layers.

## 2.3 Switching Mechanism

The electric measurement is setup for Pt/HfO<sub>2</sub>/TiN cell in Figure 2.1. The top electrode Pt is biased and bottom electrode (TiN) is grounded in DC measurement and pulsed measurement. And the observed current-voltage (I-V) characteristics show that the device perform threshold switching behavior in Figure 2.3. During cycle 1, device can turn on at one threshold voltage with value of around 5V and keep low resistance state under 0.5 nA compliance current. While the applied voltage is removed, the device turns off and goes back to initial high resistance state. And the overlap of next 6 cycles I-V curves with cycle 1 verifies this threshold switching's occurrence. This DC voltage sweep is obtained by using semiconductor parameter analyzer (Hewlett-Packard, HP4145B) at room temperature.

The pulsed measurement is also applied on our device by Agilent 81110A PG pulse generator. And during measurement, the Pt layer is biased and the bottom electrode is connected to the channel 2 of OSC. Figure 2.4 shows the pulse switching behavior of Pt/HfO<sub>2</sub>/TiN cell and a circuit diagram of pulse measurement system. And some delay time is needed for device turn on and also some relaxation time is needed for device turn off as Figure 2.4(b) shown. Based on

seniors' work [7-8], this switching performance is attributed to the electron trapping during transport from cathode to anode under positive voltage. The traps in  $\text{HfO}_2$  layer is empty under no bias condition. Then positive voltage is applied on top electrode, the electrons are injected from TiN and fill the empty trap sites in  $\text{HfO}_2$  layer, which owns about 0.7eV trap energy below the conduction band. After a certain amount of filled traps, electron transport suddenly increase and device switches to low resistance state. When the outside voltage is removed, the electron prefers going back to cathode due to the difference of work function between two metal electrodes, which results in the detrapping of electrons from trap sites and make device get back to high resistance state. This electron transport certainly needs time, which shows as delay time and relaxation time in the end. And during the electron trapping / detrapping processes, the compliance current plays an role of controlling the total amount of injected electrons from cathode. Furthermore, that make PHT<sup>②</sup> device could perform the resistance switching under relatively higher value of  $I_{CC}$  in some case[7-8].

To look into this electron transport process, some literature shows the possible way to simply the mechanism[9-10]. After excluding

---

□ Pt/ $\text{HfO}_2$ /TiN

the possibility of Schottky emission and F-N tunneling, also ignoring the directly tunneling from cathode to anode due to 10 nm thick oxide layer, the trap-assisted-tunneling becomes the main reason for the electron's sudden increase transport, which is shown in Figure 2.5. Under positive bias, the electrons are injected from TiN electrode, which is subject to compliance current, as shown Pc step. Then the injected electrons can be transported by two differed ways,  $P_{T1}$ , which is that electrons emission into the conduction band and then go to neighboring traps; or  $P_{T2}$ , which is the electron tunneling between traps. Both of them are temperature involved. And finally the step of Pa is processed, electrons tunneling into anode from traps. These simplified four-step-process for electron transport can help to understand the stochastic performance in switching behavior. The tunneling probability of one electron and its transmission rate can be calculated based on N.F.Mott's theory[11]. Here for  $P_{T1}$  and  $P_{T2}$ , the electron tunneling probabilities can be computed by the following equations:

$$P_{T1}: P_1 = P_0 \cdot \exp\left(-\frac{E_t}{KT}\right); P_{T2}: P_2 = P_0 \cdot \exp\left(-\frac{2R}{\xi}\right); P_0 = \text{constant}. \quad (2.1)$$

Here  $\xi$  is the electron wave function localization length, and usually 0.3 nm for  $\text{HfO}_2$ , and  $E_t$  is the trap energy below the conduction band,

which is 0.7eV as mentioned before; the distance between traps R has a scope, 0.3~0.6 nm.

For 10 nm thick HfO<sub>2</sub> layer, P<sub>2</sub> is always larger than P<sub>1</sub>, which means that P<sub>T2</sub> always occurs more than P<sub>T1</sub>. Furthermore, the process can be reduced into three-step transport, P<sub>C</sub>, P<sub>T2</sub>, and P<sub>a</sub> for simplification. By using the same consideration in [10], which is to treat each trap as a single-mode oscillator bedded in the dielectric matrix, the tunneling rate of electron between traps (P<sub>T2</sub>) has a formation of

$$\bar{\nu} = \frac{\sqrt{\pi}\hbar W_T}{m^*D^2Q_0\sqrt{KT}} \cdot \exp\left(-\frac{W_{opt}-W_T}{2KT}\right) \cdot \exp\left(-\frac{2D\sqrt{2m^*W_T}}{\hbar}\right) \cdot \exp\left(-\frac{eFD}{2KT}\right) \quad (2.2)$$

Here the  $W_T$  is the minimum energy required for electrons to escape from trap,  $W_{opt}$  is the optical ionization energy,  $F$  is the electric field,  $D$  is the distance between one trap and its neighbor trap[10]. It is shown that P<sub>T2</sub> is a thermally stimulated process, and related with distance between one trap and its neighbor trap. as we know, the distance between traps certainly is a random value determined by various conditions, such as the previous turn-off process, temperature and the electron injection from TiN electrode. So it is reasonable to think the random delay and relaxation come from the P<sub>T2</sub> step.

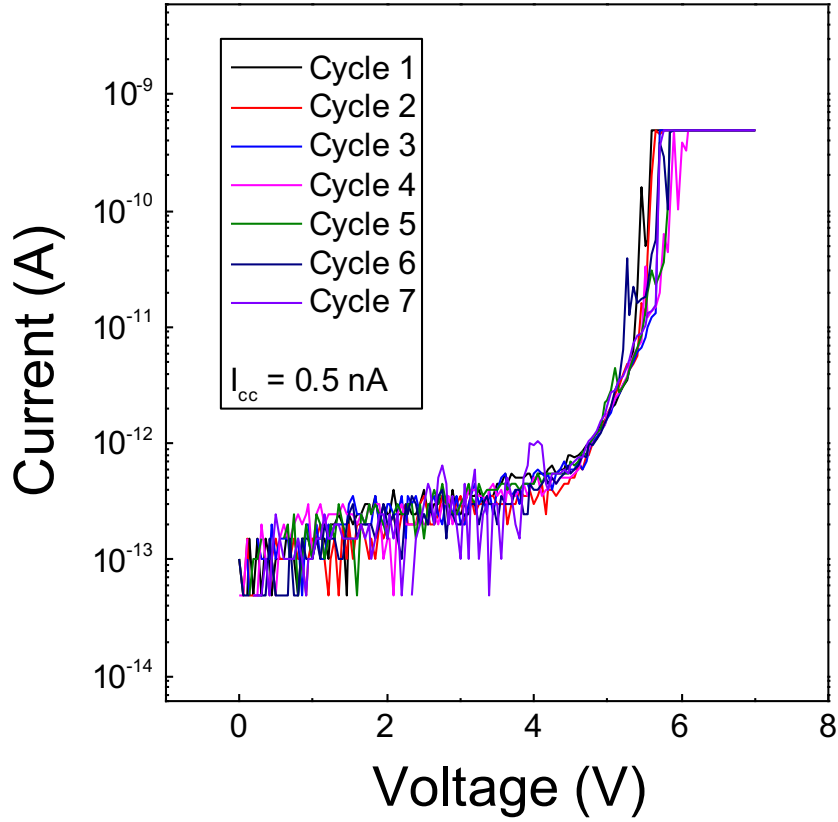


Figure 2.3. I-V curves under compliance current  $I_{cc}=0.5$  nA of PHT device. Cycle 1 shows the typical threshold switching behavior with a threshold voltage around 5V; and the next 6 cycles overlaps the cycle 1, verifying the occurrence of threshold switching of Pt/HfO<sub>2</sub>/TiN cell with a 10nm thick oxide layer.



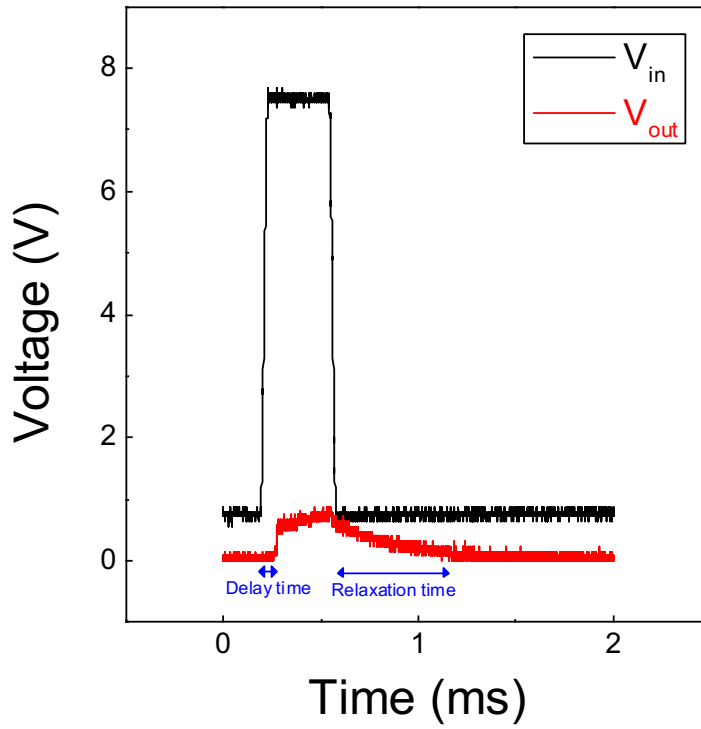
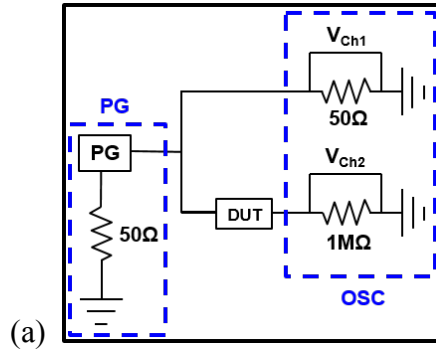


Figure 2.4. (a) circuit diagram of pulse measurement system; (b) pulse switching performance of PHT device with diagram of measurement system. After one input pulse is applied on the device, the memristor turns on after a short delay time, also one small relaxation time is needed for cell to change back to high resistance state, just like the read curve shows.

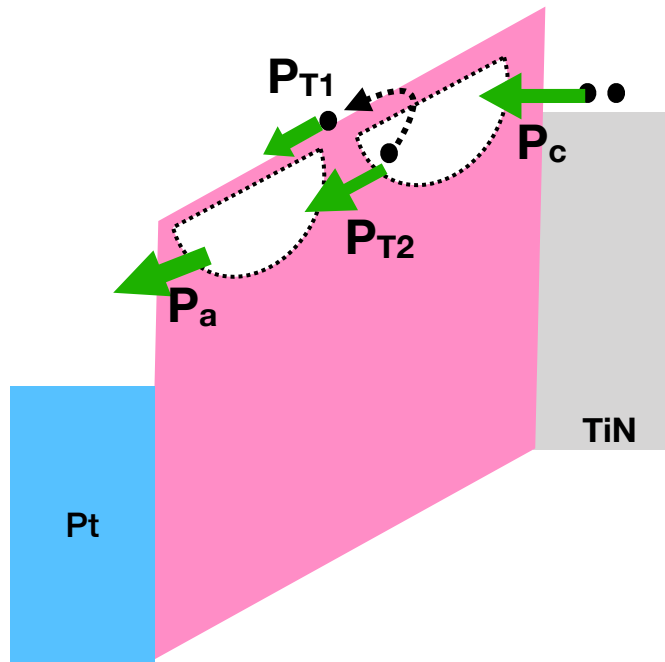


Figure 2.5. The simplified trap-assisted-tunneling process in PHT device.  $P_c$  step: the electrons are injected from TiN electrode;  $P_{T1}$  step: electrons emission into the conduction band and then go to neighboring traps;  $P_{T2}$  step: the electron tunneling between traps.  $P_a$  step: electrons tunneling into anode from traps.

## 2.4 Experimental Verification and Results

By measuring the delay time of PHT device under different temperatures and voltages, which is shown in Figure 2.6, we observed that with higher temperature the delay time decreases due to increased thermal speed of electrons[11–12], and also, as mentioned above in KAN<sup>③</sup>'s work[10], the transmission rate has a formula like equation (2.2), the activation energy  $\frac{W_{opt}-W_T}{2KT}$ , which needs to overcome for electron tunneling, also gets lower with increased temperature. And the effect of trap density may also contribute for this decrease in delay time.

Moreover, when we increase applied voltage, the drift velocity of electrons gets higher, that leads to decrease in delay time, and if we keep increase the voltage, the distribution become narrower, and reaches certain saturation. That's because that there are sufficient electrons for filling all traps, so the thermal detrapping or any kind of detrapping of trapped electrons could not affect the whole transport. Meanwhile, the drift velocity of electrons cannot keep increasing with voltage, in the end it has one saturation value[13]. For relaxation time of PHT device, as the group work in [7] shows, it is

---

□ K. A. Nasyrov

independent of voltage, and the effect of temperature also has not been observed.

It is verified that electron transportation of Pt/HfO<sub>2</sub>/TiN memristor mainly is attributed to trap-assisted-tunneling process. And the trap-assisted-tunneling mechanism is related with temperature and distance between intrinsically existed traps in oxide layer, which might be the primary reason for its stochastic delay time and relaxation time. The cell show threshold switching behavior under a low compliance current due to limited the number of total injected electrons.

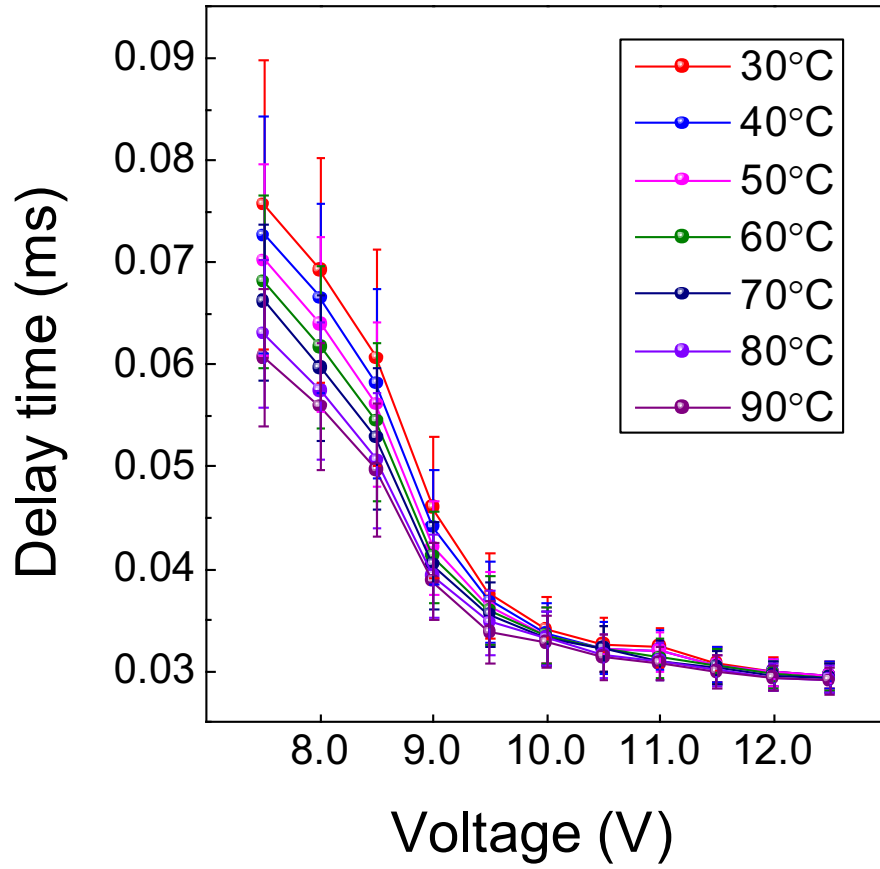


Figure 2.6. The distribution of delay time under different temperatures and voltages in the PHT device. For relaxation time of PHT device, which is shown somewhere else[7], it is independent of voltage, and the effect of temperature also has not been observed.

## 2.5 Summary

The memristor with Pt/HfO<sub>2</sub>/TiN structure in Figure 2.1 is fully studied. The TiN layer with 50 nm thickness as bottom electrode is deposited by using one sputtering system, one 10 nm HfO<sub>2</sub> layer is fabricated by ALD thermal atomic layer deposition as oxide film, the top electrode, Pt layer, is deposited by electron-evaporation to 50 nm thickness.

The threshold switching behavior of this PHT device comes from the insufficient electrons transportation. Under a relatively low compliance current, the positive voltage is applied on top electrode, the electrons are injected from TiN and fill the empty trap sites in HfO<sub>2</sub> layer. After a certain amount of filled traps, electron transport suddenly increase and device switches to low resistance state. When the outside voltage is removed, the electron prefers going back to cathode due to the difference of work function between two metal electrodes, which results in the detrapping of electrons from trap sites and makes device get back to high resistance state. This electron transport certainly needs time, which shows as delay time and relaxation time in the end. And during the electron trapping / detrapping processes, the compliance current plays an role of controlling the total amount of injected electrons from cathode.

By measuring the delay time of PHT device under different temperatures and voltage shown in Figure 2.6, it is observed that with higher temperature the delay time decreases due to increased thermal speed of electrons[10], the transmission rate has a formula like equation (2.2), the activation energy  $\frac{W_{opt}-W_T}{2KT}$ , which needs to overcome for electron tunneling, also gets lower with increased temperature. And the effect of trap density may also contribute for this decrease in delay time. Moreover, with increasing applied voltage the drift velocity of electrons gets higher, that leads to decrease in delay time, and if we keep increase the voltage, the distribution become narrower, and reaches certain saturation. That's because that there are sufficient electrons for filling all traps, so the thermal detrapping or any kind of detrapping of trapped electrons could not affect the whole transport. Meanwhile, the drift velocity of electrons cannot keep increasing with voltage, in the end it has one saturation value[13]. For relaxation time of PHT device, as the group work in [7] shows, it is independent of voltage, and the effect of temperature also has not been observed.

The electron transportation of this Pt/HfO<sub>2</sub>/TiN memristor, which is explained by trapping / detrapping process, mainly is attributed to trap-assisted-tunneling process. And the trap-assisted-tunneling mechanism is related with temperature and distance between

intrinsically existed traps in oxide layer, resulting in its stochastic delay time and relaxation time.



## Chapter 3. Random Number Generator

### 3.1. Introduction

As existing random number generators, Pseudo-random number generator (PRNG) and True-random number generator (TRNG) show very different properties. Usually PRNG strongly depends on its algorithms or codes, which result in the easy attack. Especially for the sequences they generate could be predictable from their seed value that is fed into the generator at the start. That makes TRNG become the main role in information security. A key or signature that is hard to guess, or closely impossible for prediction, is considered as random. So usually one sufficient entropy source that contains the randomness from the natural world is supplied to the generator, mostly PRNG. This entropy source works as randomness source for generator and leads to the true random number. In other word, the quality of the entropy source for random number generator decides how hard to guess the output sequence.

Modern TRNG has similar structure, such as the Intel's TRNG in[14]. It consists of an entropy source, followed by digitization to make the raw noise become random data with high quality, and one health testing zone to check for potential failure of the entropy source, last these sequences may go into some entropy pool with

higher conditions, and finally the bits will be used for seeding certain generator, which in Intel' TRNG is DRBG, to output abundant random bits for system. So as we see, the true random number is generated from a combination structure. To solve the limit of the bit generation rate, usually the entropy source is fed into some TRNG and then connected with PRNG circuit to expand the output.

PRNG , as mentioned above, commonly has one or more inputs seed value to generate pseudorandom numbers. The seed owns unpredictability and come from certain nature noise or the other kind of true randomness source. Linear Feedback Shift Register (LFSR) is a one kind of PRNG type circuit. It will generate random bits based on its seed value and the feedback connection.

### **3.2. Pseudo-Random Number Generator (PRNG)**

A key or signature that is hard to guess, or closely impossible for prediction, is considered as random. From one point of view, the PRNG contains three types of functions. The initialization function to digitize the entropy source, then the transformation function to process the change or repetition of state, at last the output function for random bits. That's why PRNG is considered as a synthesis of pure mathematical algorithm and only "pseudo-random". Usually

PRNG strongly depends on its algorithms or codes, which result in the easy attack. Especially for the sequences they generate could be predictable from their seed value that is fed into the generator at the start. However, under properly construction of algorithm or codes, PRNG could show more random and unpredictable than natural random noise, that's why many cryptographic systems still use and strength the PRNG to generate key stream.

For PRNG structure, the highly dependence of functions result in its pseudo randomness due to highly developed hacker's technique. So its randomness basically comes from the seed, and transmission by its construction. Like in LFSR, the D-flip-flop will pass this randomness to the next state and embody it in output bits.

### 3.3. D Flip-Flop

The D flip-flop is one kind of flip-flops, whose output is strongly dependent with a new clock cycle. The classical positive-edge-triggered D flip-flop is used in this paper. It captures the value of D-input at the rising edge of each new clock and the captured value becomes the Q output with some delay time, like Figure 3.1 shows, the change of input before the next clock coming will be ignored. As

its truth table shows in Figure 3.2, the D flip-flop also can be seen as the delay line, which transmits the input values after some delay.

Flip-flops form the basis of shift register and the D flip-flop that is used for this paper is constructed with MOS P-Channel and N-Channel mode devices in a single monolithic structure. When the delivery of data from one stage to the next with the processing of positive-going clock signal, a reset process also can be done by Reset line in it.

The D flip-flop used in this paper is MC14015B dual 4-bit static shift register from ON Semiconductor company. Each register has independent clock and reset inputs with a single serial data input[26].

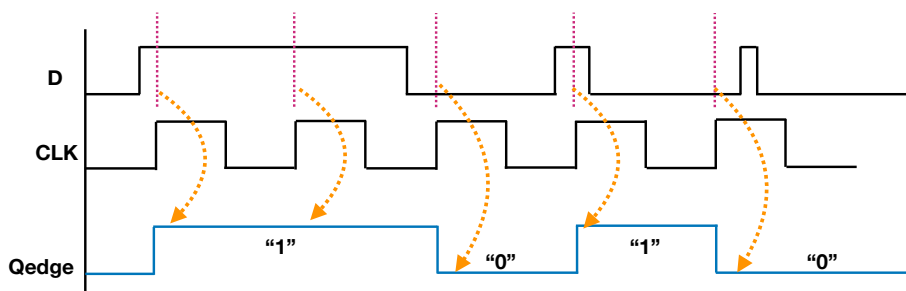


Figure 3.1. The work principle of positive-edge-triggered type of D flip-flop. “1” means logic 1, “0” means logic 0 in binary system. CLK is the clock input, Qedge is the output of D flip-flop.

	Clock	D	Qnext
	Rising edge	0	0
	Rising edge	1	1
X	Non-Rising	x	Q

Table 3.2. The true table of D flip-flop.

### 3.4. Linear Feedback Shift Register

The Linear Feedback Shift Register is one shift-register whose input is a linear function of its previous states[15]. It is usually constituted by D flip-flops and XOR logic gates. And there are two kinds of LFSR classified by the connection way of XOR gates, the external feedback type and internal feedback type, or known as Fibonacci and Galois LFSR, respectively. In this paper, the Fibonacci LFSR is used. The differences of these two kinds with the same feedback function are value of seed and order of tap. Tap is the bit position that influenced the next state and its order represents the number of LFSR's stages. Here is 3-stage Fibonacci LFSR as example shown in Figure 3.3, and its feedback connection is

$$G(X) = X^3 + X^2 + 1 \quad (3.1)$$

This feedback function means that the second and third state are sent back into the input after the XOR operation, So any LFSR can be represented by feedback function in Figure 3.5 with the formula of

$$G(X) = g_m X^m + g_{m-1} X^{m-1} + g_{m-2} X^{m-2} \dots g_2 X^2 + g_1 X + g_0 \quad (3.2)$$

The feedback connection can be understood by seeing the circuit from the point of view of modulo-2 mathematical algorithm, in which

the XOR operation is equal with the addition operation. The coefficient of  $G(X)$  function is the order of tap and its value represents the connection state with XOR logic gate. If the tap is connected with the XOR gate, the corresponding coefficient is 1, otherwise 0. The choice of taps that is connected with XOR gates determines how many values we will get in a sequence before the output repeats, like Figure 3.4 shows, the output sequence of LFSR will start over after one period. There is one choice of feedback connection to lead to the longest sequence and shows the most random possibility for output bits, and the maximal length is  $2^n - 1$  for  $n$ -stage LFSR, 7 turns for 3-stage LFSR in Figure 3.4.

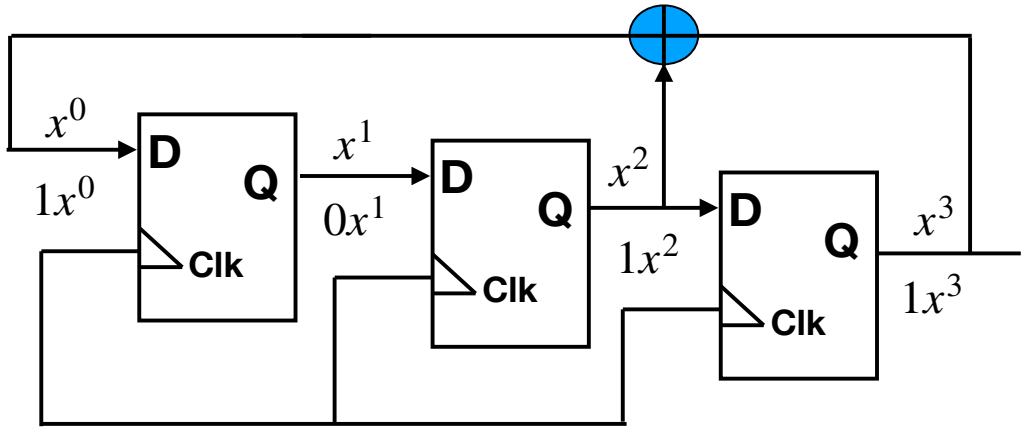


Figure 3.3. The 3-stage Fibonacci LFSR with feedback of  $G(X) = X^3 + X^2 + 1$ . The order of taps is shown as  $x^0, x^1, x^2, x^3$ . And the coefficients of them is showing the connection state with the XOR gate. If one tap is connected with XOR, its coefficient is 1, otherwise is 0.



Iteration	Q1	Q2	Q3
Seed	1	0	0
1	0	1	0
2	1	0	1
3	1	1	0
4	1	1	1
5	0	1	1
6	0	0	1
7	1	0	0

Table 3.4. The maximal period of 3-stage LFSR. Here the seed value is 001, meaning that one high voltage pulse is sent into D1 to start the LFSR.

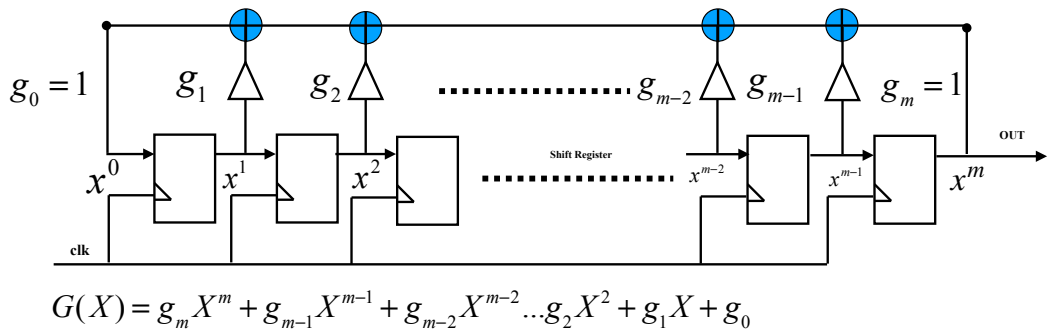


Figure 3.5. The feedback function of m-stage Fibonacci LFSR of  $G(X) = g_m X^m + g_{m-1} X^{m-1} + g_{m-2} X^{m-2} \dots g_2 X^2 + g_1 X + g_0$ . The order of taps is shown as  $x^0, x^1 \dots x^{m-1}, x^m$ . And the coefficients of them is showing the connection state with the XOR gate, represented as  $g^0, g^1 \dots g^{m-1}, g^m$ . If one tap is connected with XOR, its coefficient is 1, otherwise is 0.

### 3.5. Non-linear Feedback Solutions for LFSR

The biggest problem of Linear Feedback Shift Register structure is the linear connection, which results in easy cryptanalysis. To solve that, a large number of designs are proposed. And from one point of view, the generally presented implementation can be classified into three kinds [28].

Like the solution shown in Figure 3.6, It has been called as Fibonacci NLFSR [28]. This type contains the number of  $n$  bits (from right to left) and a state feedback which comes from every bit and goes into  $n - 1$ th bit. With clock signal advancing, the new input of bit  $n - 1$  is calculated by certain non-linear function of previous values of all other bits. This measure is strongly dependent on the choice of non-linear function.

The second way to strengthen complexity is to combine several LFSRs by feeding their outputs into a non-linear function[30][31]. The linear complexity of strengthened new generator also deeply depends on non-linear function's choice. As one case shown in Figure 3.7, the Geffe generator consists of three LFSRs and one two-to-one multiplexer [29], whose output is presented by

$$b(t) = a_3(t) \oplus \overline{a_1(t)} (a_2(t) \oplus a_3(t)). \quad (3.3)$$

Its linear complexity is an overall value depending on the degrees of feedback polynomials of these three LFSRs. In other words, the unpredictability of new generator is synthesis of unpredictability of all the used LFSRs, even higher.

Besides various nonlinear feedback transformation , the third solution is to use the irregular clocking in LFSR [29], shown in Figure 3.8 and Figure 3.9. The Massey–Rueppel’s generator in Figure 3.8 enhances the complexity of feedback by setting the LFSRs at two different clocks. This multispeed system leads to output of

$$c(t) = \sum_{i=0}^{l-1} a(t+i)b(dt+i). \quad (3.4)$$

Here  $d$  is a secret variable, which decides the clock of LFSR-2 is  $d$  times as fast as clock of LFSR-1 . For the example in Figure 3.9, the clock of LFSR-2 is subject to the output of LFSR-1 through one AND gate, which means the available situation for LFSR-2 to change state at time  $t$  is the LFSR-1’s output  $a_1(t-1) = 1$ . This situation leads to different clock frequency for these two LFSRs by controlling clock pulses. And then with a proper organization of the degrees of these three LFSRs, the linear complexity of outputs does increase.

These three solutions restructure the implementation of LFSR to enhance the linear complexity. However, they still have some defects. The Fibonacci NLFSR suffers from long propagation time

due to large feedback function and low statistical properties. The other have problems of coincidence probability to reduce the security. In spite of these deficiency, these examples show the basic idea to solve the main shortage of LFSR , the strong linear feedback function.

These three solutions provide the basic idea of how to transform the LFSR structure to increase the complexity of its feedback. And based on that, one new transformation of LFSR is proposed.

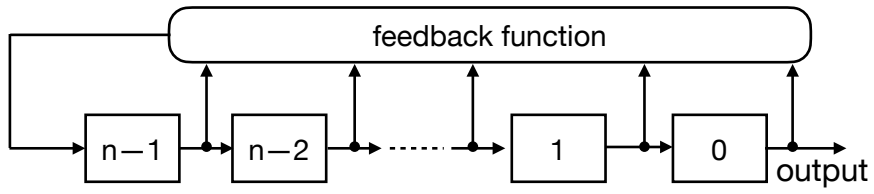


Figure 3.6. An  $n$ -bit Fibonacci NLFSR, adapted from[28].

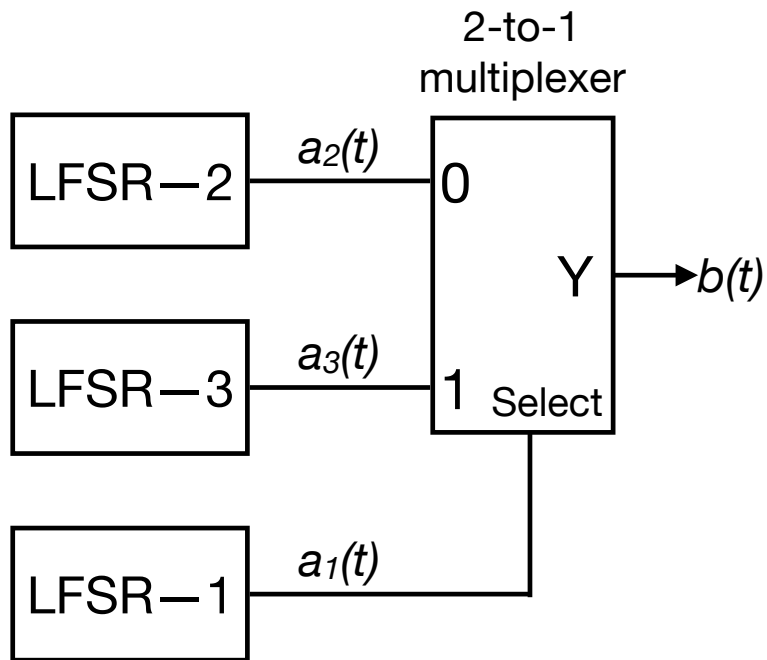


Figure 3.7. The Geffe generator, adapted from[29].

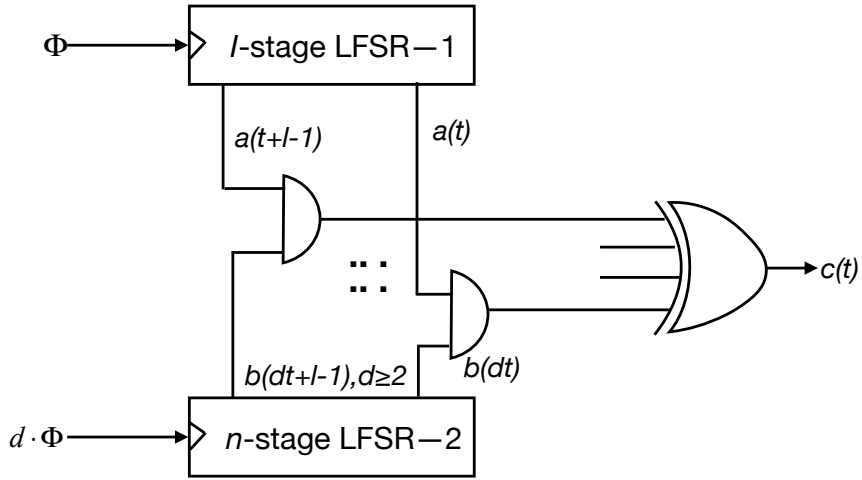


Figure 3.8. The Massey-Rueppel's generator, adapted from[29].

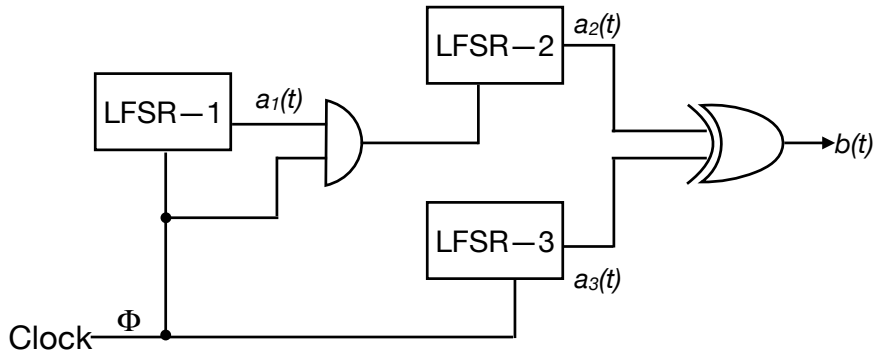


Figure 3.9. The Beth-Piper stop-and-go generator, adapted from[29].

### 3.6. True Random Number Generator

Modern TRNG has similar structure, such as the Intel's TRNG in[14]. It consists of an entropy source, followed by digitization to make the raw noise become random data with high quality, and one health testing zone to check for potential failure of the entropy source, last these sequences may go into some entropy pool with higher conditions, and finally the bits will be used for seeding certain generator, which in Intel' TRNG is DRBG, to output abundant random bits for system. So, the true random number is generated from a combination structure. To solve the limit of the bit generation rate, usually the entropy source is fed into some TRNG and then connected with PRNG circuit to expand the output.

True random number generator depends on the sufficient entropy source that contains the randomness from the natural world , which will be supplied to the circuit part of PRNG. This entropy source works as the randomness source for generator and leads to the true random number[1]. In other word, the quality of the entropy source for random number generator decides how hard to guess the output sequence. And this entropy source can be understood as randomness source, or source of unpredictable behavior, it can be collected from your computer systems or noise from the surrounding, which has



true randomness[3–5]. That’s why TRNG is also called as hardware random number generator.

### 3.7. Summary

A key or signature that is hard to guess, or closely impossible for prediction, is considered as random. However, PRNG is strongly dependent on the algorithms or codes of its structure, which result in the easy attack. So TRNG becomes the main role in information security.

Modern TRNG reveals more complex structure. Usually one sufficient entropy source that contains the randomness from the natural world is supplied to the generator, mostly PRNG. The involvement of PRNG part in TRNG is mostly to solve the limit of quantity of output bits and expand to satisfy many different applications. This entropy source works as randomness source for generator and leads to the true random number. In other word, the quality of the entropy source for random number generator decides how hard to guess the output sequence.

The Linear Feedback Shift Register (LFSR) is fully studied as the most common structure in the generation of pseudo-random number.

LFSR is usually constituted by D flip-flops and XOR logic gates, whose input is a linear function of its previous states[15]. The main part of this structure is its feedback connection, which results in the repetition of the longest turn of pseudo random output. The biggest problem of Linear Feedback Shift Register structure is also the linear connection, which results in easy cryptanalysis. To solve that and break the repetition of output, a large number of designs are proposed. Based on these three solutions as stated above, the restructuring of feedback connection in LFSR is implemented in next chapter.

## Chapter 4. TRNG using Pt/HfO<sub>2</sub>/TiN memristor

### 4.1. Introduction

As mentioned above, memristor can show resistive switching behavior under proper bias conditions, however, the nonuniformity has troubled people to push the next generation memory. This kind of chaos in switching performance results from the stochastic physical characteristics and other complex mechanisms. Nevertheless, considering the true random number generator at hardware level, stochastic phenomena could be used as the certain entropy source if proper design is proposed. That is exactly what we pursue. The Pt/HfO<sub>2</sub>/TiN memristor show a large change scale in switching parameters, which is a big problem for memory application, however, a great superiority in area of random number generator. The new circuit is designed for take full advantage of its random change in delay time and relaxation time. By using the Linear Feedback Shift Register (LFSR), which is commonly applied for PRNG, one best fit project is got. And this best befitting design provides enough output bits for NIST randomness test. Moreover, a meritorious result is shown as evidence to indicate that the PHT memristor is a great candidate for random number generator as the entropy source. This proposed TRNG provide the simple structure

and shows great advantage in high compatibility with CMOS fabrication standard[18–21]. It is evidential to say that Pt/HfO<sub>2</sub>/TiN memristor is a good candidate for true random number generator circuit implementation.

## 4.2. Design and Simulation

The proposed new TRNG circuit is shown in Figure 4.1. In this new design, memristor can serve as the certain entropy source. The Pt/HfO<sub>2</sub>/TiN memristor show a large change scale in switching parameters, which becomes a great superiority in the application of the random number generator. By using Linear Feedback Shift Register, one best fit project is got to take full advantage of its random change in delay time and relaxation time. The LFSR used in this design is 4-stage LFSR as shown in Figure 4.2. Its maximal period of output, which can be seen as pseudo random number, is shown in Table 4.3 according to its linear feedback connection,

$$G(X) = X^4 + X^3 + 1. \quad (4.1)$$

And through the simulation result, it is found that the small change in feedback function of original LFSR is also achieved. Through the simulation, the true table of new design is observed by monitoring the marked points in circuit, shown in Figure 4.4 (b). If the

memristor's output is 1, the feedback signal keeps the same with the original LFSR, otherwise the feedback becomes the reversion value. In other words, the feedback will reverse at the edge of change of memristor's output, which is same as feeding the new seed to the chain of D flip-flops at every cycle of input in memristor.

This stops the repetition of output sequences of LFSR, and make us get the new cycle of random bits all the time. However, that makes the choice of clock frequency and the width of input pulse a little difficult. After many considerations, a proper clock (16 KHZ) and a pulse with width of  $350\mu s$  is applied in the real experiment.

The simulation is made on LTspice, which is a high performance SPICE simulation software, schematic capture and waveform viewer with enhancements and models for easing the simulation of analog circuits. The simulation circuit diagram is Figure 4.5, in which the memristor is represented by one resistance for simplification. The MOSFET structure of this new TRNG circuit is shown in Figure 4.6. M1, M2 and M3 form the AND gate, M4 and M5 compose the NOR gate, M6, M7, M8 and M9 constitute the XOR gate. Here M4 with R3 work as NMOS inverter, only memristor's output and the feedback value at the same moment are logic "1", the output of the AND gate is 1. For the NOR gate, the inputs become previous output of the AND gate and memristor's output, only both of them show low

voltage, it output logic “1”. This output with feedback value from LFSR become input of the XOR gate. Finally, the new feedback is sent into the first D flip-flop in chain of the LFSR. The randomness of memristor transmits from AND M1 to the NOT gate part in XOR gate, at last is sent into LFSR as seed.

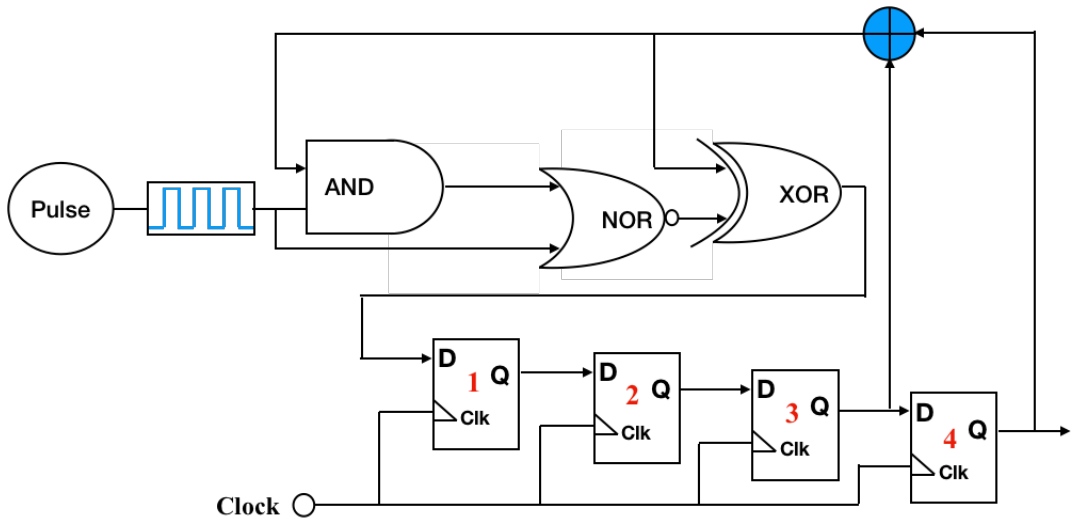


Figure 4.1. The proposed new circuit of TRNG based on the PHT memristor. When memristor's output and the feedback value at the same moment are logic "1", the output of the AND gate is 1. For the NOR gate, the inputs become previous output of the AND gate and memristor's output, only both of them show low voltage, it output logic "1". This output with feedback value from LFSR become input of the XOR gate. Finally, the new feedback is sent into the first D flip-flop in chain of the LFSR.

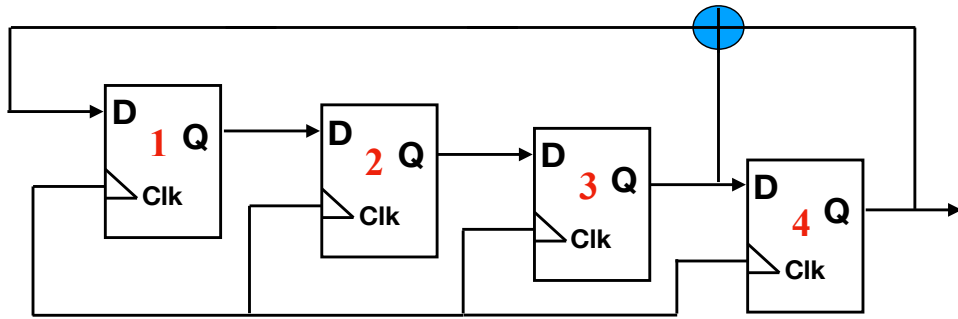
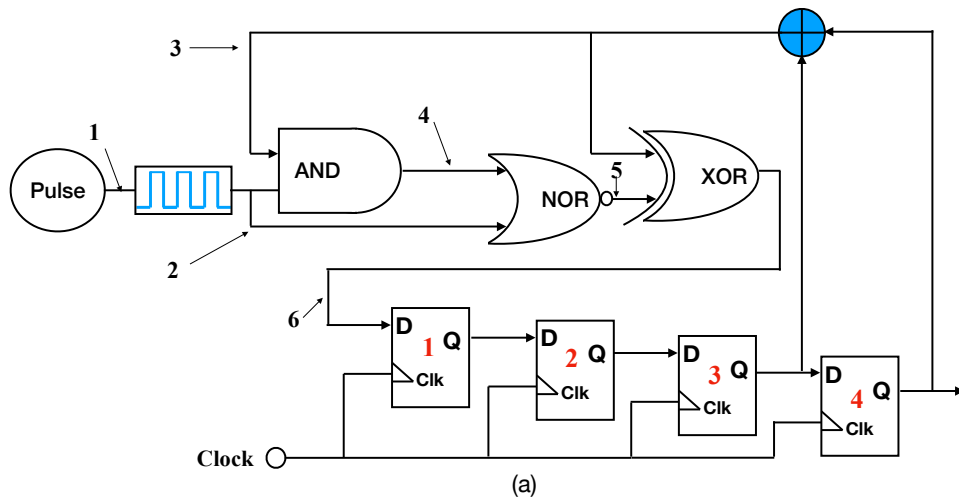


Figure 4.2. The schematic form of 4-stage LFSR used in our TRNG with a feedback function as  $G(X) = X^4 + X^3 + 1$ .



CLK	Q1	Q2	Q3	Q4
1st	1	0	0	0
2nd	0	1	0	0
3rd	0	0	1	0
4th	1	0	0	1
5th	1	1	0	0
6th	0	1	1	0
7th	1	0	1	1
8th	0	1	0	1
9th	1	0	1	0
10th	1	1	0	1
11th	1	1	1	0
12th	1	1	1	1
13th	0	1	1	1
14th	0	0	1	1
15th	0	0	0	1
16th	1	0	0	0

Table 4.3. The longest turn of original 4-stage LFSR based on its feedback function of  $G(X) = X^4 + X^3 + 1$ .



Old feedback (3)	Memristor (2)	AND (4)	NOR (5)	XOR (6)	New feedback (6)
0	0	0	1	1	1
0	1	0	0	0	0
1	0	0	1	0	0
1	1	1	0	1	1

(b)

Figure 4.4. (a) the monitoring point of the new circuit of TRNG based on PHT memristor; (b) the true table of function in proposed TRNG. In (a) point 1 is showing the waveform of input pulse, point 2 is the output of the memristor, the point 3 can show the form of old feedback signal the point 4 is monitoring the output of AND and point 5 is for NOR, the point 6 shows the new feedback that will be sent into LFSR chain.

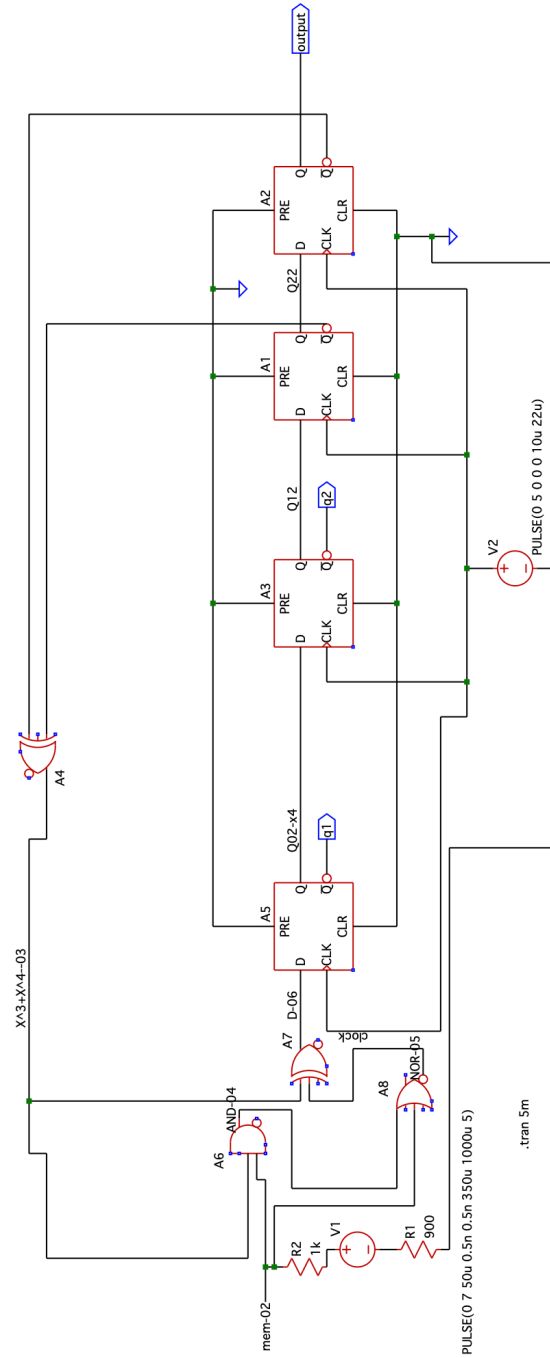


Figure 4.5. The simulation circuit diagram in LTspice of the proposed TRNG. This simulation is practiced to test and verify the feedback function of restructured LFSR, so here the memristor is represented as resistance R2 just for simplification. And as true table shows, there are 6 points under monitoring.

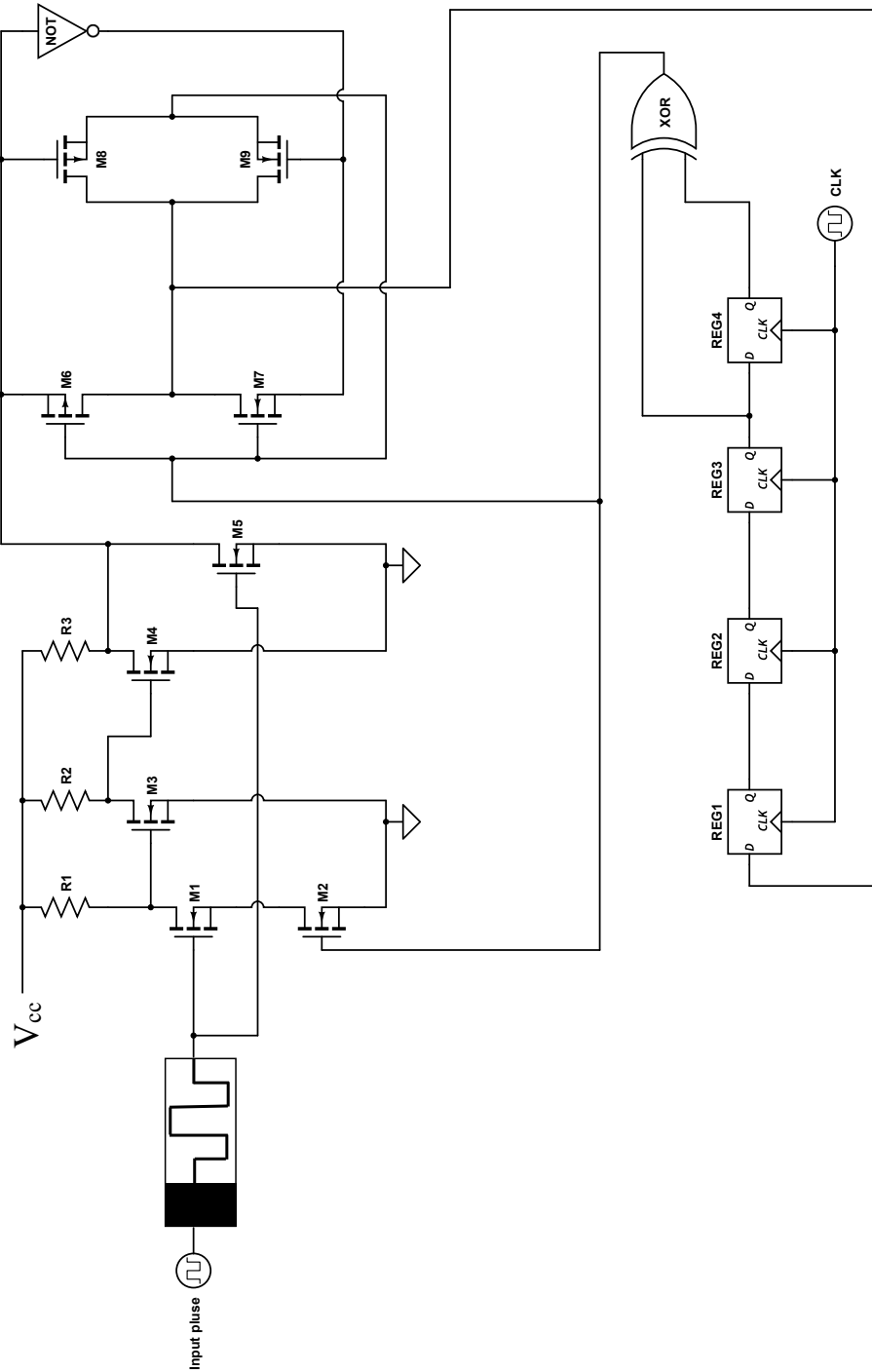


Figure 4.6. The MOSFET structure of proposed TRNG. M1, M2 and M3 form the AND gate, M4 and M5 compose the NOR gate, M6, M7, M8 and M9 constitute the XOR gate. And LFSR is consist of 4 registers and one XOR gate with clock setting.

### 4.3. Experimental Procedure

In the real experiment, the designed circuit is fabricated on breadboard and the TRNG is realized on the Probe station 2 equipment, as shown in left of Figure 4.7. The Probe station 2 (from Alessi, with model of REL 5500) contains the one semiconductor parameter analyzer (Hewlett–Packard, 4145B), one Agilent 81110A Pulse generator, oscilloscope (Tektronix, TDS 684C) and one available temptronic, thermal chuck.

AND gate is Quad 2–input AND gate with product number of SN74LS08N; NOR gate of HD74HC02P is Quad 2–input NOR gate from Renesas Technology; XOR gate is Quad 2–input exclusive–OR gate of 74HCT86 from Nexperia; and D flip–flop is come from the Dual 4–bit static shift register MC14015B of On Semiconductor[26]. The connection of each gate is shown as right in Figure 4.7.

After implementation of circuit on breadboard, the output of memristor , which is put on the chuck (marked in brown), was sent in to the position in the breadboard following the design. And the output of LFSR in breadboard was sent into oscilloscope for collection and observation. The experimental output waveform is shown in Figure 4.9. Also the clock is set to 16 KHZ and a pulse with width of  $350\mu s$  is applied on memristor device,  $600\mu s$  between two input pulses to

let PHT device totally turn off. The rise and fall time of pulse is  $25\ \mu s$ .

Also, the dynamic change of voltage level at every marked point in proposed TRNG is shown in Figure 4.8. The monitoring point 1 is showing the waveform of input pulse, point 2 is the output of the memristor marked in red, the point 3 can show the form of old feedback signal, which is marked in blue. The point 4 is monitoring the output of AND marked in green gate and point 5 is for NOR marked in orange, the point 6 shows the new feedback that will be sent into LFSR chain, marked in purple.

The random delay and relaxation time from monitoring point 2 determine the random position of LFSR to change the cycle in monitoring point 3. And also the new seed will be fed into LFSR to start outputting shown monitoring point 6, just same as the simulation result in the last chapter. The blue waveform in monitoring point 3 is signal from old feedback function, while the purple one in monitoring point 6 is new feedback result. The difference between old feedback and new feedback is already stated above in truth table of circuit, here in Figure 4.8, this difference is more vivid and obvious. As we see, when the memristor's output is 1, the feedback signal of monitoring point 6 keeps the same with the original LFSR, monitoring point 3; when the memristor's output is 0, the feedback of point 6

becomes the reversion value of feedback from point 3. That is to say the feedback will reverse at the edge of change of memristor's output, which is same as feeding the new seed to the chain of D flip-flops at every cycle of input in memristor, just same with the simulation result above.

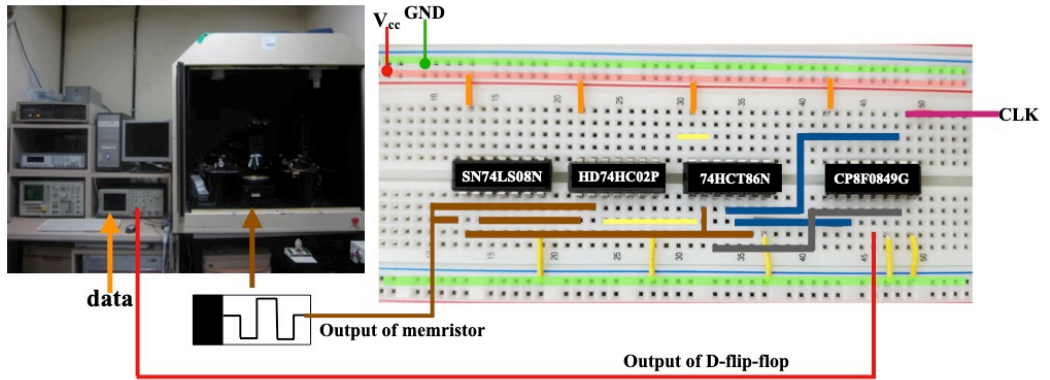


Figure 4.7. The real implementation of proposed TRNG on the breadboard (right) and Probe station 2 (left). The breadboard is EIC-104J solderless breadboard with board of  $165 \times 110 \times 8.5 \text{ mm}$  and 2 terminal strips. The Probe station 2 (from Alessi, with model of REL 5500) contains the one semiconductor parameter analyzer (Hewlett-Packard, 4145B), one Agilent 81110A Pulse generator, oscilloscope (Tektronix, TDS 684C) and one available temptronic, thermal chuck.



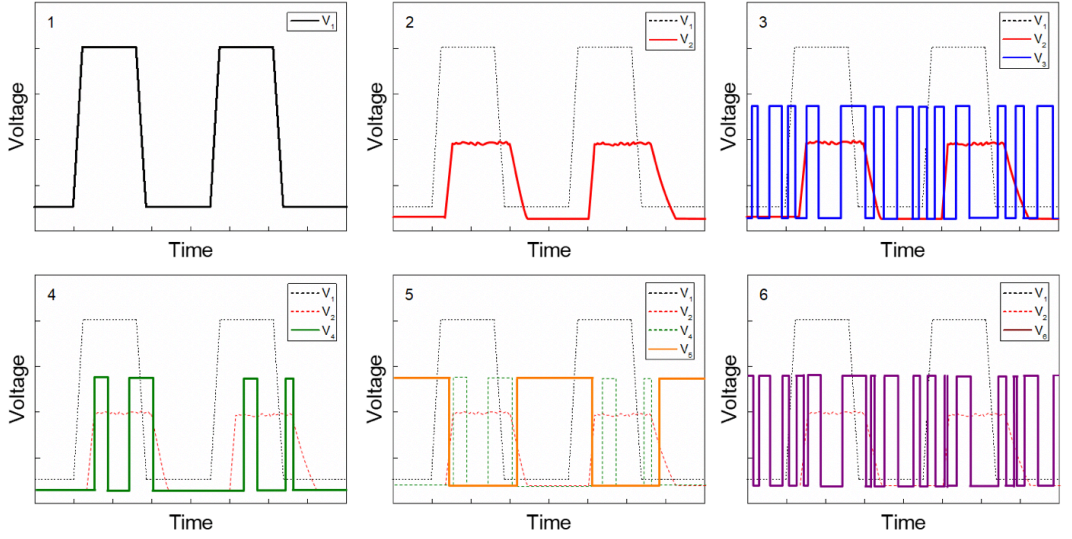


Figure 4.8. the work principle of proposed TRNG , which is from the point of view of dynamic change of voltage level. The monitoring point 1 is showing the waveform of input pulse, point 2 is the output of the memristor marked in red, the point 3 can show the form of old feedback signal marked in blue, the point 4 is monitoring the output of AND marked in green gate and point 5 is for NOR marked in orange, the point 6 shows the new feedback that will be sent into LFSR chain, marked in purple.

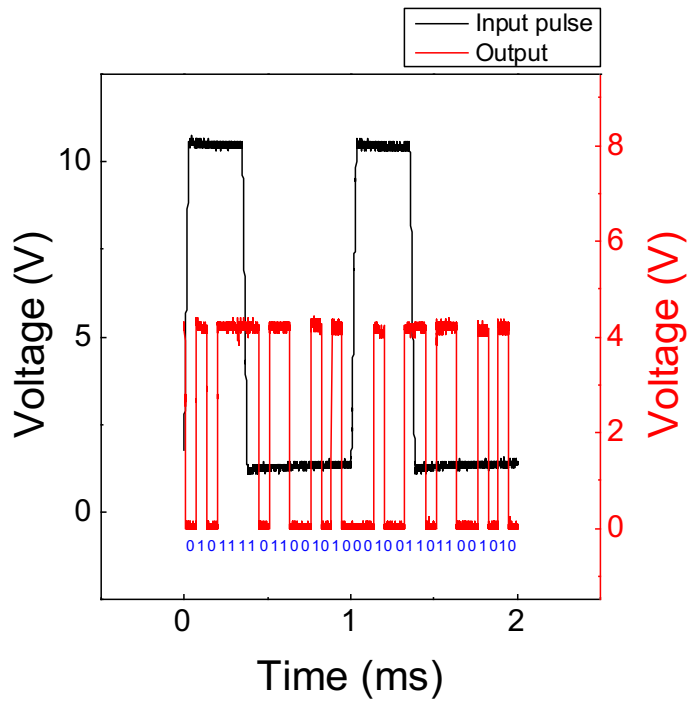


Figure 4.9. Experimental output waveform of proposed TRNG, which is from oscilloscope of Probe Station 2. The output of two input pulses, and the output can be read as the number marked in blue in the unit of clock pulse.

## 4.4. NIST Randomness Tests

NIST has published one statistical test suite for random and pseudorandom number generator, which contain some criteria for characterizing the generator[6]. There are 15 tests in it for testing randomness of binary bit streams, which are used to determine the feasibility of generator for cryptography. And the 15 tests are designed under the consideration of three standard conditions: ① uniformity; ② scalability; ③ consistency. And this statistical test suite determines certain sequence random or not by the value of P-value. The value of P-value is “1” means that particular sequence has perfect randomness. Usually only the comparison of p-value with significance level of your collected data makes sense. The significance level depends on the amount of your collected bits. So if the p-value of one sequence for one test, is higher than this significance level, then that particular sequence passes this test. That is the way for NIST to judge some sequence. In our experiment, a data bit stream with length  $n=1,000,000$  was set for each test. And total 90 sequences were collected to run the whole tests, which could provide the enough bits for each test and get results with high accuracy. And with 90 sequences, a confidence level of 95.5% is acceptable and a P-value higher than 0.001 would result in a pass for certain test. Also same with other paper, the test is run under one

null hypothesis, that the bit streams collected from the new TRNG circuit are random. The definition and mathematical principles are explained as below according to[6][27].

#### 4.4.1 Frequency Test

This Frequency test is the primary test of all, it's recommended that to run the Frequency test at first. If some sequence does not pass the Frequency test, neither does it pass any other tests. The purpose of this test is to find out whether the number of zeros is equal to the number of ones, which is saying that the proportion of zeros or ones should be 0.5[6]. The P-value of Frequency test is calculated by equation:

$$P = \text{erfc}\left(\frac{S_{obs}}{\sqrt{2}}\right), \quad (4.1)$$

$\text{erfc}(i)$  is the complementary error function.

Here  $S_{obs}$  is the test statistic for the input sequence( $\epsilon$ ) with length  $(n)$ :  $S_{obs} = \frac{|S_n|}{n}$ .

#### 4.4.2 Frequency within a Block Test

The purpose of this test is to determine the number of ones in an M-bit block, especially comparing to the expected frequency under

the assumption of random input, around  $M/2$ . So the first step of this test is to divide the  $n$  bit stream input into  $N = \left\lfloor \frac{n}{M} \right\rfloor$  block,  $M$  is the length of each block[6].

Then the proportion of ones in each block is calculated by equation :

$$\pi_i = \frac{\sum_{j=1}^M \varepsilon_{(i-1)M+j}}{M}, \text{ for } 1 \ll i \ll N. \quad (4.2)$$

And later how much this value is close to the 0.5 is determined by :

$$\chi^2(obs) = 4M \sum_{i=1}^N (\pi_i - 1/2)^2 ; \quad (4.3)$$

And  $P = igamc\left(\frac{N}{2}, \frac{\chi^2(obs)}{2}\right)$ , here  $igamc(i)$  is defined as incomplete gamma function.

### 4.4.3 Run Test

The purpose of this test is to determine whether the number of runs of ones and zeros of various lengths is as expected for our assumption of random inputs. By observing the oscillation between zeros and ones, too fast or too low, to pursue the long run of either ones or zeros, where the run is an uninterrupted sequence[6]. the P-value is computed by following equations:

The test statistic:

$$V_n(obs) = \sum_{K=1}^{n-1} r(K) + 1; \quad r(K) = \begin{cases} 0 & \text{if } \varepsilon_K = \varepsilon_{K+1} \\ 1 & \text{otherwise} \end{cases}. \quad (4.4)$$

Finally the P-value will be got by:

$$P = \operatorname{erfc}\left(\frac{|V_n(obs) - 2n\pi(1-\pi)|}{2\sqrt{2n\pi(1-\pi)}}\right), \quad (4.5)$$

$\operatorname{erfc}(i)$  is the complementary error function.

#### 4.4.4 Test for Longest Run of Ones in a Block

This test pursues the longest run of ones in a block with length M. the purpose is to determine whether the length of longest run of ones in input sequence match with the same assumption of random sequence[27]. For our input sequences, the value of 128 is chosen for block length. So the frequencies of the longest runs in each block will hold the following counts:

$v_i$	Run length
$v_0$	$\leq 4$
$v_1$	5
$v_2$	6
$v_3$	7
$v_4$	8
$v_5$	$\geq 9$

Then the P-value will be computed by equation:

$$P = igamc(\frac{K}{2}, \frac{\chi^2(obs)}{2}), \quad (4.6)$$

$$\text{here } \chi^2(obs) = i = \sum_{i=0}^K \frac{(v_i - N\pi_i)^2}{N\pi_i}, \quad (4.7)$$

$igamc(i)$  is the incomplete gamma function. Also, parameters are set as M=128, K=5, N=49.

#### 4.4.5 Binary Matrix Rank Test

The purpose of this test is to check for the linear dependence within the fixed length substrings of the original sequence. the number of rows in each matrix M is set to 32, the number of columns in each matrix is set to 32, the number of matrix is  $N = \left\lfloor \frac{n}{MQ} \right\rfloor$  [6].

The P-value is calculated by equation:

$$P = e^{-\chi^2(obs)/2}. \quad (4.8)$$

#### 4.4.6 Discrete Fourier Transform Test

The purpose is to detect the periodic characteristics in input sequences[6]. It will convert the bit-stream into spectral graph to determine if there are any high peaks exceeding the 95% threshold and the number of these peaks is different than 5%. So firstly it will compute the equation on each bit of input:

$x_i = 2\varepsilon_i - 1$ , to change zero and one into -1 and +1.

Then the P-value will be calculated by:

$$d = \frac{(N_1 - N_0)}{\sqrt{n(.95)(.05)/4}}; \quad (4.9)$$

$$P = \text{erfc}\left(\frac{|d|}{\sqrt{2}}\right). \quad (4.10)$$

#### 4.4.7 Non-overlapping Template Matching Test

The purpose is to check that if the generator produce too many occurrences of a given target strings[6]. So there will be one target string with length m to be provided. And the P-value is computed by :

$$\chi^2(obs) = \sum_{j=1}^N \frac{(W_j - \mu)^2}{\sigma^2}; \quad (4.11)$$

$$P = \text{igamc}\left(\frac{N}{2}, \frac{\chi^2(obs)}{2}\right). \quad (4.12)$$

N, the number of independent block is set to 8 in this test.

#### 4.4.8 Overlapping Template Matching Test

The purpose is similar with the Non-overlapping Template Matching test. It focuses on the occurrences of the given target strings by using m-bit window to search for a certain m-bit pattern[6]. So its P-value is calculated by

$$\chi^2(obs) = \sum_{i=0}^5 \frac{(v_i - N\pi_i)^2}{N\pi_i}; \quad (4.13)$$

$$P = \text{igamc}\left(\frac{5}{2}, \frac{\chi^2(obs)}{2}\right). \quad (4.14)$$



#### 4.4.9 Maurer's "Universal Statistical" Test

The purpose of this test is to see if the input sequence can be significantly condensed without loss of information[6]. It will detect the number of bits between matching patterns. There are three parameters in this test,  $L$ ,  $Q$ ,  $n$ , respectively representing the length of each block, the number of blocks in the initial sequence and the length of bit string. Its P-value is computed by :

$$P = \text{erfc} \left( \left| \frac{f_n - \text{expectedValue}(L)}{\sqrt{2}\sigma} \right| \right), \quad f_n = \frac{1}{K} \sum_{i=Q+1}^{Q+K} \log_2(i - T_j). \quad (4.15)$$

Here the *expectedValue*( $L$ ) and  $\sigma$  are from the table of precomputed values, which is related with the chosen initialization segment.

#### 4.4.10 Linear Complexity Test

The purpose of this test is to look for the sequence that is complex enough to be considered as random, especially comparing the output with the same commensurable linear feedback shift register (LFSR)[6]. That's why this test is particularly important in our case. It will indicate that whether our circuit restructure is successful or

not. The input sequence is divided into independent N blocks of M bits. The P-value is computed by equations:

$$\chi^2(obs) = \sum_{i=0}^6 \frac{(v_i - N\pi_i)^2}{N\pi_i}; \quad (4.16)$$

$$P = igamc\left(\frac{6}{2}, \frac{\chi^2(obs)}{2}\right). \quad (4.17)$$

The input  $\chi^2(obs)$  is a measure of how well the observed number of occurrences of fixed length LFSRs matches the expected number of occurrences under an assumption of randomness.

#### 4.4.11 Serial Test

The serial test is similar with the Frequency test, it's to check the frequency of m-bit patterns and compare them to the expected number for an assumed random sequence [6]. In other words, it will check whether the number of occurrences of the  $2^m$  m-bit overlapping patterns is approximately the same as the assumption. If m=1, then it will totally become the Frequency test in 4.4.1.

In this test, one measure,  $\nabla\psi_m^2(obs)$  and  $\nabla^2\psi_m^2(obs)$ , is used for checking how well the observed frequencies of m-bit patterns match the expected value. Finally, the P-value of Serial test is got by equation:

$$P_1 = igamc(2^{m-2}, \nabla \psi_m^2); P_2 = igamc(2^{m-3}, \nabla^2 \psi_m^2). \quad (4.18)$$

#### 4.4.12 Approximate Entropy Test

This test is similar with Serial test, it's to check the frequency of all possible overlapping  $m$ -bit patterns in the whole sequence and compare frequency of  $m$ -bit and  $(m + 1)$ -bit strings with the expected number for an assumed random sequence[6]. The input will be used for creating the exact  $n$  overlapping  $m$ -bit sequences by appending  $m - 1$  bit from the beginning to the end of the input. Then the frequency of each  $m$ -bit number that happens is numbered from all  $n$  blocks, and is also shown as  $\#i, the i \in (0, 2^m - 1)$ .

The ratio of each number to  $n$  is computed by

$$C_i^m = \frac{\#i}{n}, \phi^{(m)} = \sum_{i=0}^{2^m-1} \pi_i \log \pi_i; \quad (4.19)$$

At last the P-value is got by equation :

$$P = igamc\left(2^{m-1}, \frac{\chi^2}{2}\right); \chi^2 = 2n[\log 2 - (\phi^{(m)} - \phi^{(m+1)})]. \quad (4.20)$$

Here  $ApEn(m) = \phi^{(m)} - \phi^{(m+1)}$  in some definition.

#### 4.4.13 Cumulative Sums Test

This test is to check whether the random walks from both ends of bit-stream deviate from the average too fast. It will focus on the maximal excursion of the random walk defined by the cumulative sum of adjusted  $(-1, +1)$  digits in the sequence. For a real random sequence, the excursions of random walks should be near zero[27]. The test statistic  $z$  is the maximum value in the set of sums. The P-value is calculated b following equations:

$$P = 1 - \sum_{K=(\frac{-n}{z}+1)/4}^{(\frac{n}{z}-1)/4} \left[ \phi\left(\frac{z(4K+1)}{\sqrt{n}}\right) - \phi\left(\frac{z(4K-1)}{\sqrt{n}}\right) \right] + \sum_{K=(\frac{-n}{z}-3)/4}^{(\frac{n}{z}-1)/4} \left[ \phi\left(\frac{z(4K+3)}{\sqrt{n}}\right) - \phi\left(\frac{z(4K+1)}{\sqrt{n}}\right) \right], \quad (4.21)$$

here  $\phi(i)$  is standard normal cumulative probability distribution function as defined in [6].

#### 4.4.14 Random Excursion Test

This test is to check the number of cycles having exactly  $K$  visits in a cumulative sum random walk[6]. A cycle of a random walk contains the sequences of steps of unit length taken at random that begin at and return to origin. Its purpose is to see whether the number of visits to some state within a cycle match with expected value. This test consists of eight tests.

So firstly it will compute the equation on each bit of input:

$x_i = 2\varepsilon_i - 1$ , to change zero and one into  $-1$  and  $+1$ .

Then the test statistic and P-value will be computed by equations:

$$\chi^2(obs) = \sum_{k=0}^5 \frac{(\nu_K(x) - J\pi_K(x))^2}{J\pi_K(x)}; \quad (4.22)$$

$$P = igamc\left(\frac{5}{2}, \frac{\chi^2(obs)}{2}\right). \quad (4.23)$$

#### 4.4.15 Random Excursion Variant Test

This test is to check the total number of times that a particular state occurs in a cumulative sum random walk and observe the difference with the expected value for a true random sequence [6]. There are eighteen tests in it for checking states from  $-9, \dots, -1$  and  $+1, \dots, +9$ .

In it, the total number of times that the state  $x$  is visited during the entire random walk is determined by  $\xi(x)$  in all  $J$  cycles. Finally the P-value is computed by

$$P = erfc\left(\frac{|\xi(x) - J|}{\sqrt{2J(4|x| - 2)}}\right). \quad (4.24)$$

The NIST standard randomness test contains above 15 kinds of test. And in these tests, the complementary error function is defined as :

$$erfc(i) = \frac{2}{\sqrt{\pi}} \int_i^{\infty} e^{-u^2} du; \quad (4.25)$$

The incomplete gamma function is defined by :

$$igamc(a, i) = \frac{1}{\Gamma(a)} \int_i^{\infty} e^{-t} t^{a-1} dt , \quad \Gamma(z) = \int_0^{\infty} t^{z-1} e^{-t} dt . \quad (4.26)$$

## 4.5. Results and Analysis

As mentioned above, memristor works as the entropy source in the new TRNG circuit, its stochastic physical characteristics are fully used by reversion of LFSR's feedback function in the new circuit. Also the 4-stage LFSR structure is used and restructured to achieve one more complex RNG circuit to avoid attacking. By using the AND gate, NOR gate and XOR gate, we have changed the strong linear feedback function. Also, the involvement of the random delay and relaxation time will make that the feedback reverse itself at each change of output of memristor. Because of random delay and relaxation time of memristor, the position of reversion occurrence is random and unpredictable from outside, which is similar with feeding the new seed value to LFSR structure before its repetition. And the output from 4-stage LFSR is collected and digitized by MATLAB coding. The binary output bits are run in NIST randomness tests. the final result is achieved as Figure 4.9 shows.

The results of NIST randomness test contain two forms of analysis, one is the proportion of sequences that pass that particular statistical test, the other is the distribution of P-values[6]. The P-value in the final result table ( Figure 4.9) is actually the result of Goodness-of-Fit Distributional Test on the all P-values, which could be understood by thinking it as P-value of P-values. And this distributed result of P-value is used to judge the uniformity of certain sequence.

The NIST result of our proposed TRNG shows a pretty high P-value of Frequency test, which is the primary evidence for random sequence under null hypothesis. And then the P-value of Linear Complexity test shows that structure of the proposed TRNG circuit indicates the stronger complexity, comparing with the original 4-stage LFSR. Also the P-value of approximately 0.6 for Entropy test also prove the randomness of entropy source from memristor. In other word, the result of NIST randomness test , which is run with collected bits, proves that our proposed TRNG is strong enough, especially the randomness of Pt/HfO<sub>2</sub>/TiN memristor is sufficient and effective.

In conclusion , the new true random number generator circuit based on the Linear Feedback Shift Register by using memristor is proposed. By using the stochastic delay and relaxation time during

the memristor switching process as the source of randomness, the output of proposed TRNG pass all 15 NIST Special Publication 800-22 randomness tests without any post-processing. And because of application of basic logic gates and LFSR's structure, our TRNG provides the simple structure and shows a great advantage in high compatibility with CMOS fabrication standard[18-21]. It is evidential to say that Pt/HfO<sub>2</sub>/TiN memristor is a good candidate for true random number generator circuit implementation.



Test	P-value	Pass rate	Minimum pass rate	pass/fail
1. Frequency test	0.189397	88/90	86/90	Pass
2. Frequency test within a block	0.107371	90/90	86/90	Pass
3. Runs test	0.911413	90/90	86/90	Pass
4. Longest Run	0.268170	87/90	86/90	Pass
5. Discrete Fourier transform test	0.407091	88/90	86/90	Pass
6. Serial test	0.050485	89/90	86/90	Pass
	0.100508	86/90	86/90	
7. Approximate entropy test	0.602458	89/90	86/90	Pass
8. Cumulative sums test	0.019334/	89/90	86/90	Pass
	0.387648	89/90		
9. Linear complexity	0.139036	88/90	86/90	Pass
10. Non-overlapping T.M.	0.076154	89/90	86/90	Pass
11. Rank	0.000259	87/90	86/90	Pass
	0.048716	59/60	57/60	
12. Random Excursions	0.399443	88/90	86/90	Pass
13. Random Excursions Variant	0.042708	89/90	86/90	Pass
14. Maurer's Universal	0.238042	86/90	86/90	Pass
15. Overlapping T.M.	0.002043	90/90	86/90	Pass

Table 4.10. The NIST randomness test result of proposed TRNG by using memristor. A data bit stream with total 90 sequences were collected to run the whole tests, a confidence level of 95.5% is applied for the interpretation, which requires at least 86 sequences pass each test. A P-value higher than 0.001 would result in a pass for certain test.

## 4.6. Summary

In this chapter, one new true random number generator circuit is designed and implemented on breadboard. The Pt/HfO<sub>2</sub>/TiN memristor show a large change scale in switching parameters, which is a great superiority in area of random number generator. The new circuit is designed for take full advantage of its random change in delay time and relaxation time. By using AND gate, NOR gate and XOR gate, we have slightly changed the strong linear feedback function of the 4-stage Linear Feedback Shift Register (LFSR) to achieve one more complex RNG circuit to avoid attacking. The main working principle is that because of random delay and relaxation time of memristor, the position of reversion occurrence is random and unpredictable from outside, which is similar with feeding the new seed value to LFSR structure before its repetition.

And enough output bits for NIST randomness test were collected from this implemented TRNG. The binary output bits are run in NIST randomness tests. The final result is achieved as Figure 4.9 shows. Moreover, all 15 standard randomness tests are passed, which is an evidence to indicate that the PHT memristor is a great candidate for random number generator as the entropy source. The interpretation of the result report of the NIST tests and explanation about how the

NIST values the randomness of sequences are also stated in this chapter.

## Chapter 5. Conclusion

### 5.1. Summary

In this work, the memristor with Pt/HfO<sub>2</sub>/TiN structure is fully studied. TiN layer with 50 nm thickness as bottom electrode, HfO<sub>2</sub> layer of 10 nm thickness is the oxide film in this structure, Pt layer is deposited to 50 nm thickness as top electrode. The threshold switching behavior of this PHT device is observed under a relatively low compliance current. When the positive voltage is applied on top electrode, the electrons are injected from TiN and fill the empty trap sites in HfO<sub>2</sub> layer. After a certain amount of filled traps, electron transport suddenly increase and device switches to low resistance state. When the outside voltage is removed, the difference of work function between two metal electrodes could lead to a opposite electric field. Under this situation, the electron prefers going back to cathode which results in the detrapping of electrons from trap sites and makes device get back to high resistance state. This electron transport also shows random delay time and relaxation time in the switching process.

In order to fully understand the mechanism of PHT device and its stochastic performance, one simplified three-step process is proposed and the measurement of the delay time of PHT device

under different temperatures and voltages was carried out. It is observed that with higher temperature the delay time decreases due to increased thermal speed of electrons, higher transmission rate and the change in trap density. With increasing applied voltage the decrease in delay time is observed due to higher drift velocity of electrons gets higher, and if we keep increasing the voltage, the distribution become narrower, and reaches certain saturation. That's because that there are sufficient electrons for filling all traps, so the thermal detrapping or any kind of detrapping of trapped electrons could not affect the whole transport. So the understanding is gained that the electron transportation of Pt/HfO<sub>2</sub>/TiN memristor is mainly attributed to trap-assisted-tunneling process. And the trap-assisted-tunneling mechanism is related with temperature and distance between intrinsically existed traps in oxide layer, and plays one important role in its stochastic delay time and relaxation time.

In Chapter 3, the relationship between true random number generator and pseudo random number generator is discussed. And the basic idea of how to transform the structure of LFSR is provided. Although the PRNG is more easily to implement, its strong dependence in algorithms leads to easy attacking. So modern TRNG is fabricated on the base of the structure of PRNG to simultaneously obtain the various magnitudes of output for different application and

higher hurdles for attacking. TRNG transmits the raw random noise into entropy source to provide the seed for random number generation. The Linear Feedback Shift Register (LFSR), as the most common structure in the generation of pseudo-random number, is usually constituted by D flip-flops and XOR logic gates. The input of LFSR is a linear function of its previous states. This linear connection also become the biggest problem of Linear Feedback Shift Register, which results in easy cryptanalysis. To solve that and break the repetition of output, the basic idea of transformation of LFSR is achieved based on the common three solutions that are proposed by many researchers.

In Chapter 4, the new true random number generator circuit is designed and implemented on breadboard. To solve the linearity of LFSR, other basic gates are used in transformation of feedback connection. By using AND gate, NOR gate and XOR gate, the slight change in the strong linear feedback function of the 4-stage Linear Feedback Shift Register (LFSR) is achieved to get one more complex RNG circuit. The main working principle is that because of random delay and relaxation time of memristor, the position of reversion occurrence is random and unpredictable from outside, which is similar with feeding the new seed value to LFSR structure before its repetition. We collect enough output bits for NIST randomness test

from this implemented TRNG. Then, the binary output bits are run in NIST randomness tests. Finally all 15 standard randomness tests are passed.

In conclusion, by using the Pt/HfO<sub>2</sub>/TiN memristor as the entropy source, one true random number generator based on transformation of linear feedback shift register structure is proposed. And this proposed TRNG presents valuable performance in NIST randomness test, indicating that the Pt/HfO<sub>2</sub>/TiN memristor is a great candidate for random number generator as the entropy source.

# Bibliography

- [1] Patrick Lacharme, Andrea Rock, Vincent Strubel, Marion Videau. **2012**, *The Linux Pseudorandom Number Generator Revisited*, <<https://hal.archives-ouvertes.fr/hal-01005441>>.
- [2] N. Heninger, Z. Durumeric, E. Wustrow and J. A. Halderman. **August 2012**, 'Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices', Proceedings of the Twenty-first USENIX Security Symposium, <<https://factorable.net/weakkeys12.conference.pdf>>.
- [3] C. S. Petrie and J. A. Connelly. **2005**, 'A noise-based IC random number generator for applications in cryptography', *IEEE Transactions On Circuits And Systems I: Fundamental Theory And Applications*, vol. 47, no. 5, pp. 615–621, doi: 10.1109/81.847868.
- [4] C. S. Petrie and J. A. Connelly. **1996**, 'Modelling and simulation of oscillator based random number generators', *IEEE International Symposium on Circuits and Systems*, vol. 4, pp. 324–327, doi: 10.1109/ISCAS.1996.541967.
- [5] Mike Hamburg, Paul Kocher and Mark E. Marson. **March 12, 2012**, *ANALYSIS OF INTEL'S IVY BRIDGE DIGITAL RANDOM NUMBER GENERATOR*, Cryptography Research, Inc., 575 Market St., 11th Floor San Francisco, CA 94105 (415) 397-0123, <[https://cdn.atraining.ru/docs/Intel\\_TRNG\\_Report\\_20120312.pdf](https://cdn.atraining.ru/docs/Intel_TRNG_Report_20120312.pdf)>
- [6] Andrew Rukhin, Juan Soto, et al. **April 2010**, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, NIST Special Publication (SP) 800-22 Rev. 1a, <<http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf>>.
- [7] Y. Wu, B. Lee, H.-S. P. Wong. **26-28 April 2010**, 'Ultra-Low Power Al<sub>2</sub>O<sub>3</sub>-based RRAM with 1μA Reset Current', Proceedings of the 2010 International Symposium on VLSI Technology, Systems, and Applications, Hsin Chu, Taiwan, < <http://toc.proceedings.com/08402webtoc.pdf>> p.136.
- [8] Shimeng Yu, Bin Gao, Haibo Dai, Bing Sun, Lifeng Liu, et al. **2010**, 'Improved Uniformity of Resistive Switching Behaviors in HfO<sub>2</sub> Thin Films with Embedded Al Layers ', *Electrochemical and Solid-State Letters*, 13(2) H36-H38, doi: 10.1149/1.3267050.
- [9] Kyung Seok Woo, Yongmin Wang, Jihun Kim, Yumin Kim, Young Jae Kwon, Jung Ho Yoon, Woohyun Kim, and Cheol Seong Hwang. **2018**, 'A True Random Number Generator Using Threshold- Switching-Based Memristors in an Efficient Circuit Design ', *Advanced Electronic Materials*, 1800543, doi: 10.1002/aelm.201800543.



- [10] Yumin Kim, Young Jae Kwon, Dae Eun Kwon, Kyung Jean Yoon, Jung Ho Yoon, Sijung Yoo, Hae Jin Kim, Tae Hyung Park, Jin Woo Han, Kyung Min Kim, and Cheol Seong Hwang. **2018**, 'Nociceptive Memristor', *Advanced Materials*, 1704320, doi: 10.1002/adma.201704320.
- [11] Shimeng Yu, Ximeng Guan, and H.-S. Philip Wong. **2011**, 'Conduction mechanism of TiN/HfO<sub>x</sub>/Pt resistive switching memory: A trap-assisted- tunneling model', *APPLIED PHYSICS LETTERS* 99, 063507, doi: 10.1063/1.3624472.
- [12] K. A. Nasyrov and V. A. Gritsenko. **2011**, 'Charge transport in dielectrics via tunneling between traps', *JOURNAL OF APPLIED PHYSICS*, 109, 093705, doi: 10.1063/1.3587452.
- [13] N.F. Mott and E. A. Davis. **1979**, *Electronic Processes in Non-Crystalline Materials*, Clarendon, Oxford, U.K., Chapter 2(P32-64), Chapter 3(P79-89).
- [14] Ajay Kumar Singh. **2008**, Retrieved 1 March ,2011, *Electronic Devices And Integrated Circuits*. PHI Learning Pvt. Ltd. pp. 77–.
- [15] Peter Y. Yu, Manuel Cardona. **2005**, *Fundamentals of Semiconductors: Physics and Materials Properties*, Springer, New York, pp. 227-228.
- [16] Mike Hamburg Paul Kocher Mark E. Marson. **March 12, 2012**. , *ANALYSIS OF INTEL'S IVY BRIDGE DIGITAL RANDOM NUMBER GENERATOR* , Cryptography Research, Inc. and Intel Corporation, <[https://cdn.atraining.ru/docs/Intel\\_TRNG\\_Report\\_20120312.pdf](https://cdn.atraining.ru/docs/Intel_TRNG_Report_20120312.pdf)>.
- [17] L. Chen and G. Gong. **2012**, *Communication System Security*, CRC Press, first edition, New York, doi: 10.1201/b12078.
- [18] Jung Ho Yoon, Seul Ji Song, Il-Hyuk Yoo, Jun Yeong Seok, Kyung Jean Yoon, Dae Eun Kwon, Tae Hyung Park, and Cheol Seong Hwang. **2014**, 'Highly Uniform, Electroforming-Free, and Self-Rectifying Resistive Memory in the Pt/Ta<sub>2</sub>O<sub>5</sub>/HfO<sub>2-x</sub>/TiN Structure', *Advanced Functional Materials*, 24, 5086, doi: 10.1002/adfm.201400064.
- [19] B. Govoreanu, G. S. Kar, Y.-Y. Chen, V. Paraschiv, S. Kubsek, A. Fantini, I. P. Radu, L. Goux, S. Clima, R. Degraeve, N. Jossart, O. Richard, T. Vandeweyer, K. Seo, P. Hendrix, G. Pourtois, H. Bender, L. Altimine, D. J. Wouters, J. A. Kittl, M. Jurczak. **December 2011**, *Presented at IEDM*, Washington, USA
- [20] P. Gonon, M. Mougnot, C. Vallee, C. Jorel, V. Jousseau, H. Grampeix, F. El Kamel. **2010**, 'Resistance switching in HfO<sub>2</sub> metal-insulator-metal devices ', *Journal of Applied Physics*, 107, 074507, doi: 10.1063/1.3357283.

- [21] Runchen Fang, Yago Gonzalez Velo, Wenhao Chen, Keith Holbert, Michael Kozicki, Hugh Barnaby, Shimeng Yu. **2014**, 'Total ionizing dose effect of  $\gamma$ -ray radiation on the switching characteristics and filament stability of  $\text{HfO}_x$  resistive random access memory', *Applied Physics Letters*, 104, 183507, doi: 10.1063/1.4875748.
- [22] Hao Jiang, Daniel Belkin, Sergey E. Savel'ev, Siyan Lin, Zhongrui Wang, Yunning Li, Saumil Joshi, Rivu Midya, et al. **2017**, 'A novel true random number generator based on a stochastic diffusive memristor', *Nature Communications*, 8, 882, doi: 10.1038/s41467-017-00869-x.
- [23] Jung Ho Yoon, Kyung Min Kim, Seul Ji Song, Jun Yeong Seok, Kyung Jean Yoon, Dae Eun Kwon, et al. **2015**, 'Pt/Ta<sub>2</sub>O<sub>5</sub>/HfO<sub>2-x</sub>/Ti Resistive Switching Memory Competing with Multilevel NAND Flash', *Advanced materials*, 27, 3811, doi: 10.1002/adma.201501167.
- [24] Kyung Min Kim, Gun Hwan Kim, Seul Ji Song, Jun Yeong Seok, Min Hwan Lee, Jeong Ho Yoon and Cheol Seong Hwang. **2010**, 'Electrically configurable electroforming and bipolar resistive switching in Pt/TiO<sub>2</sub>/Pt structures', *Nanotechnology*, 21, 305203, doi: 10.1088/0957-4484/21/30/305203.
- [25] Kyung Min Kim, Byung Joon Choi, Min Hwan Lee, Gun Hwan Kim, Seul Ji Song, Jun Yeong Seok, Jeong Ho Yoon, Seungwu Han and Cheol Seong Hwang. **2011**, 'A detailed understanding of the electronic bipolar resistance switching behavior in Pt/TiO<sub>2</sub>/Pt structure', *Nanotechnology*, 22, 254010, doi: 10.1088/0957-4484/22/25/254010.
- [26] ON Semiconductor. **2005**, 'Dual 4-Bit Static Shift Register', MC14015B, <<https://www.onsemi.com/pub/Collateral/MC14015B-D.PDF>>.
- [27] Filip Veljković, Vladimir Roz'ić and Ingrid Verbauwhede. **12-16 March 2012**, 'Low-Cost Implementations of On-the-Fly Tests for Random Number Generators', Proceedings of the Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, doi: 10.1109/DATE.2012.6176635.
- [28] Elena Dubrova, Maxim Teslenko and Hannu Tenhunen. **March 2008**, 'On Analysis and Synthesis of (n,k)-Non-Linear Feedback Shift Registers', Proceedings of the 2008 Design, Automation and Test in Europe, Munich, Germany, doi: 10.1109/DATE.2008.4484856.
- [29] Kencheng Zeng, Chung-Huang Yang, Dah-Yea Wei, and T.R.N. Rao. **1991**, 'Pseudo-random bit generators in stream-cipher cryptography', *Computer*, 24, 2, doi: 10.1109/2.67207.

[30] M.J.B. Robshaw. **1995**, *Stream ciphers*, Tech. Rep. TR - 701, RSA Laboratories, <<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.30.2991&rep=rep1&type=pdf>>.

[31] Yuriy Tarannikov. **2001**, 'New constructions of resilient Boolean function with maximum nonlinearity', *Lecture Notes in Computer Science*, vol. 2355, pp. 66–77, <[https://link.springer.com/content/pdf/10.1007/3-540-45473-X\\_6.pdf](https://link.springer.com/content/pdf/10.1007/3-540-45473-X_6.pdf)>.

[32] W. Meier and O. Staffelbach. **1989**, 'Fast correlation attacks on certain stream ciphers', *J. Cryptol.*, vol. 1, no. 3, pp. 159–176.

# Abstract in Korean

Internet of Things (IoT) 와 같은 새로운 기술은 민감한 정보를 처리하기 때문에 보안 문제를 많은 관심을 끌고 있다. 이를 해결하기 위한 방법으로 난수 (random number) 가 쓰인다. 난수 생성기는 개인 정보 보호에서 중요한 역할을 하고 있다. 왜냐하면 난수 생성기는 모든 사람에게 전용의 서명을 만들 수 있기 때문이다. 의사 난수 (pseudo random number)는 수학 알고리즘을 통해서 생성될 수 있고 보통 씨앗 값 (seed) 등 조건이 필요하다. 그래서 생성 조건이나 씨앗 값이 같다면 그 결과값은 항상 같다. 그리고 현재 시간에 생성된 난수를 통해서 다음 순간의 난수도 알 수 있다. 그러므로 인공적인 난수 (의사 난수) 보다 순수 난수는 더 많은 주목을 받고 있다. 순수 난수 생성기 (True Random Number Generator) 는 설비나 사용 환경에 존재하고 있는 물리적 순수 추정 과정을 이용해서 순수 난수를 만든다. 그래서 순수 난수는 공격 저항력을 강화된다.

Compliance current 상대적으로 낮을 때, Pt / HfO<sub>2</sub> / TiN 멤리스터 (memristor) 는 threshold switching 나타내면서 무작위 delay time 과 relaxation time 볼 수 있다. 따라서 Pt / HfO<sub>2</sub> /

TiN 메모리를 이용하고 Linear Feedback Shift Register 바탕으로  
순수 난수 생성기를 새로 만들었다.

이 순수 난수 생성기에서 Pt / HfO<sub>2</sub> / TiN 멤리스터는 entropy  
source 맡기며 씨앗 값을 제공한다. 이 Pt / HfO<sub>2</sub> / TiN  
멤리스터의 무작위 스위칭 파라미터는 trap-assisted-tunneling  
mechanism 통해 설명될 수 있다. 제안한 순수 난수 생성기에서  
생긴 데이터는 모든 표준 기술 연구소 (NIST) 의 무작위  
테스트를 통과하고 Pt / HfO<sub>2</sub> / TiN 멤리스터는 하드웨어 보안  
어플리케이션을 위한 완벽한 후보가 될 것을 확인했다.

주요어 : 순수 난수 생성기, Linear Feedback Shift  
Register, 멤리스터, 저항 변화 소자  
학 번 : 2017-23058

왕용민

